JEFATURA DE GABINETE DE MINISTROS

SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA

SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN

OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN

Disposición 1/2015

Bs. As.,19/2/2015

VISTO el Expediente CUDAP: EXP-JGM: 0030261/2014 del Registro de la JEFATURA DE GABINETE DE MINISTROS, el Decreto N° 378 del 27 de abril de 2005, la Decisión Administrativa N° 669 del 20 de diciembre de 2004, la Resolución N° 45 del 24 de junio de 2005 de la entonces SUBSECRETARÍA DE LA GESTIÓN PÚBLICA, la Disposición N° 6 del 8 de agosto de 2005 y Disposición N° 3 del 27 de agosto de 2013 de la OFICINA DE TECNOLOGÍAS DE INFORMACIÓN, y

CONSIDERANDO:

Que el Decreto N° 378/2005 aprobó los Lineamientos Estratégicos que deberán regir el Plan Nacional de Gobierno Electrónico y los Planes Sectoriales de Gobierno Electrónico de los Organismos de la ADMINISTRACIÓN PÚBLICA NACIONAL a fin de promover el empleo eficiente y coordinado de los recursos de las Tecnologías de la Información y las Comunicaciones.

Que la Decisión Administrativa N° 669/2004 de la JEFATURA DE GABINETE DE MINISTROS estableció en su artículo 1° que los organismos del Sector Público Nacional comprendidos en el artículo 7° de la citada medida deberán dictar o bien adecuar sus políticas de seguridad de la información conforme a la Política de Seguridad Modelo a dictarse dentro del plazo de CIENTO OCHENTA (180) días de aprobada dicha Política de Seguridad Modelo.

Que el artículo 8° de la mencionada decisión administrativa, facultó al entonces señor SUBSECRETARIO DE LA GESTIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS a aprobar la Política de Seguridad Modelo y a dictar las normas aclaratorias y complementarias de la citada medida, pudiendo dicha autoridad delegar en el DIRECTOR NACIONAL DE LA OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN las facultades aludidas.

Que consecuentemente con ello, el artículo 1° de la Resolución N° 45/2005 de la entonces SUBSECRETARÍA DE LA GESTIÓN PÚBLICA hoy SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS facultó al señor DIRECTOR NACIONAL de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN de la entonces SUBSECRETARÍA DE GESTIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS a aprobar la “Política de Seguridad de la Información Modelo” y dictar las normas aclaratorias y complementarias que requiera la aplicación de la Decisión Administrativa N° 669/2004.

Que la Disposición N° 620/2005 de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN de la entonces SUBSECRETARÍA DE GESTION PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS en su artículo 1° aprobó la “Política de Seguridad de la Información Modelo” ordenada por la Decisión Administrativa N° 669/2004, y que sirvió como base para la elaboración de las respectivas políticas a dictarse por cada organismo alcanzado por la citada norma.

Que la Disposición N° 3/2013 de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN de SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS en su artículo 1° aprobó la ‘‘Política de Seguridad de la Información Modelo” que reemplazó y actualizó a los mismos fines a la que fuera aprobada por Disposición ONTI N° 6/2005.

Que atento al incremento en cantidad y variedad de amenazas y vulnerabilidades que rodean a los activos de información, la “Política de Seguridad Modelo” oportunamente aprobada requiere ser actualizada a fin de mantener su vigencia y nivel de eficacia.

Que la mera elaboración por parte de los organismos de políticas de seguridad no es suficiente para garantizar la seguridad de la información, la que permite a su vez, garantizar la prestación continua e ininterrumpida de los diversos servicios públicos prestados por dichos organismos.

Que sólo a través de la efectiva implementación de las medidas contempladas en dichas políticas se podrá proteger acabadamente los recursos de información de los organismos como así también la tecnología utilizada para su procesamiento.

Que la presente medida se dicta en ejercicio de las facultades conferidas por el artículo 1° de la Resolución N° 45/2005 de la entonces SUBSECRETARÍA DE LA GESTIÓN PÚBLICA actual SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS.

Por ello,

EL DIRECTOR NACIONAL
DE LA OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN
DISPONE:

ARTÍCULO 1° — Apruébase la “Política de Seguridad de la Información Modelo”, que reemplaza a los mismos fines a la aprobada por Disposición ONTI N° 3/2014, que como Anexo I forma parte integrante de la presente.

ARTÍCULO 2° — Instrúyase a los organismos del Sector Público Nacional comprendidos en el artículo 7° de la Decisión Administrativa N° 669/2004 de la JEFATURA DE GABINETE DE MINISTROS, a implementar las medidas adoptadas en sus respectivas políticas de seguridad de la información dentro del plazo de CIENTO OCHENTA (180) días de publicada la presente.

ARTÍCULO 3° — Comuníquese, publíquese, dese a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese. — PEDRO JANICES, Director Nacional, Oficina Nacional de Tecnologías de Información.

ANEXO I

Política Modelo de Seguridad de la Información

INDICE

Contenido

7.2.1 Control: Responsabilidad de la dirección

7.2.2 Control: Concientización, formación y capacitación en seguridad de la información

7.2.3 Control: Proceso disciplinario

7.3 Categoría: Cese del empleo o cambio de puesto de trabajo

7.3.1 Control: Responsabilidad del cese o cambio

7.3.2 Control: Devolución de activos

7.3.3 Control: Retiro de los derechos de acceso

8. Cláusula: Gestión de Activos

8.1 Categoría: Responsabilidad sobre los activos

8.1.1 Control: Inventario de activos

8.1.2 Control: Propiedad de los activos

8.1.3 Control: Uso aceptable de los activos

8.2 Categoría: Clasificación de la información

8.2.1 Control: Directrices de clasificación

8.2.2 Control: Etiquetado y manipulado de la información

8.3 Categoría: Gestión de medios

8.3.1 Control: Administración de Medios Informáticos Removibles

8.3.2 Control: Eliminación de Medios de Información

8.3.3 Control: Seguridad de los Medios en Tránsito

9. Cláusula: Gestión de Accesos

9.1 Categoría: Requerimientos para la Gestión de Acceso

9.1.1 Control: Política de Gestión de Accesos

9.1.2 Control: Reglas de Gestión de Acceso

9.2 Categoría: Administración de Gestión de Usuarios

9.2.1 Control: Registración de Usuarios

9.2.2 Control: Gestión de Privilegios

9.2.3 Control: Gestión de Contraseñas de Usuario

9.2.4 Control: Administración de Contraseñas Críticas

9.2.5 Control: Revisión de Derechos de Acceso de Usuarios

9.3 Categoría: Responsabilidades del Usuario

9.3.1 Control: Uso de Contraseñas

9.4 Categoría: Control de Acceso a Sistemas y Aplicaciones

9.4.1 Control: Política de Utilización de los Servicios de Red

9.4.2 Control: Camino Forzado

9.4.3 Control: Autenticación de Usuarios para Conexiones Externas

9.4.4 Control: Autenticación de Nodos

9.4.5 Control: Protección de los Puertos (Ports) de Diagnóstico Remoto

9.4.6 Control: Subdivisión de Redes

9.4.7 Control: Acceso a Internet

9.4.8 Control: Conexión a la Red

9.4.9 Control: Ruteo de Red

9.4.10 Control: Seguridad de los Servicios de Red

9.5 Categoría: Control de Acceso al Sistema Operativo

9.5.1 Control: Identificación Automática de Terminales

9.5.2 Control: Procedimientos de Conexión de Terminales

9.5.3 Control: Identificación y Autenticación de los Usuarios

9.5.4 Control: Sistema de Administración de Contraseñas

10. Cláusula: Criptografía

10.1 Categoría: Cumplimiento de Requisitos Legales

10.1.1 Control: Política de Utilización de Controles Criptográficos

10.1.2 Control: Cifrado

10.1.3 Control: Firma Digital

10.1.4 Control: Servicios de No Repudio

10.1.5 Control: Protección de claves criptográficas

10.1.6 Control: Protección de Claves criptográficas: Normas y procedimientos

11. Cláusula: Física y Ambiental

11.1 Categoría: Áreas Seguras

11.1.1 Control: Perímetro de seguridad física

11.1.2 Control: Controles físicos de entrada

11.1.3 Control: Seguridad de oficinas, despachos, instalaciones

11.1.4 Control: Protección contra amenazas externas y de origen ambiental

11.1.5 Control: Trabajo en áreas seguras

11.1.6 Control: Áreas de acceso público, de carga y descarga

11.2 Categoría: Seguridad de los equipos

11.2.1 Control: emplazamiento y protección de equipos

11.2.2 Control: Instalaciones de suministro

11.2.3 Control: Seguridad del cableado

11.2.4 Control: Mantenimiento de los equipos

11.2.5 Control: Seguridad de los equipos fuera de las instalaciones

11.2.6 Control: Reutilización o retiro seguro de equipos

11.2.7 Control: Retirada de materiales propiedad del organismo

11.2.8 Control: Políticas de Pantallas Limpias

11.2.9 Control: Políticas de Escritorios Limpios

12. Cláusula: Seguridad en las Operaciones

12.1 Categoría: Procedimientos y Responsabilidades operativas

12.1.1 Control: Documentación de los Procedimientos Operativos

12.1.2 Control: Cambios en las Operaciones

12.1.3 Control: Planificación de la Capacidad

12.1.4 Control: Separación de entornos de desarrollo, pruebas y operacionales

12.2 Categoría: Protección contra el malware (código malicioso)

12.2.1 Control: Control contra el malware (código malicioso)

12.2.2 Control: Código Móvil

12.3 Categoría: Resguardo (backup)

12.3.1 Control: Resguardo de la Información

12.4 Categoría: Registro y Monitoreo

12.4.1 Control: Registro de eventos

12.4.2 Control: Protección del registro de información

12.4.3 Control: Registro del Administrador y del Operador

12.4.4 Control: Sincronización de Relojes

12.5 Categoría: Control de Software Operacional

12.5.1 Control: Instalación de software en sistemas operacionales

12.6 Categoría: Administración de vulnerabilidades técnicas

12.6.1 Control: Administración de vulnerabilidades técnicas

12.6.2 Control: Restricciones en la instalación de software

12.7 Categoría: Consideraciones sobre la auditoría de los sistemas de información

12.7.1 Control: Controles de auditoría de los sistemas de información

13. Cláusula: Gestión de Comunicaciones

13.1 Categoría: Gestión de la Red

13.1.1 Control: Redes

13.1.2 Control: Seguridad de Servicio de red

13.2 Categoría: Transferencia de información

13.2.1 Control: Procedimientos y controles de intercambio de la información

13.2.2 Control: Acuerdos de Intercambio de Información

13.2.3 Control: Seguridad de la Mensajería

13.2.4 Control: Acuerdos de confidencialidad

14. Cláusula: Adquisición, desarrollo y mantenimiento de sistemas

14.1 Categoría: Requerimientos de Seguridad de los Sistemas

14.1.1 Control: Análisis y Especificaciones de los Requerimientos de seguridad

14.1.2 Control: Seguridad de servicios aplicativos en redes públicas

14.1.3 Control: Protección de servicios de aplicativos

14.2 Categoría: Seguridad en los Sistemas de Aplicación

14.2.1 Control: Validación de Datos de Entrada

14.2.2 Control: Controles de Procesamiento Interno

14.2.3 Control: Autenticación de Mensajes

14.2.4 Control: Validación de Datos de Salidas

14.3 Categoría: Seguridad de los Archivos del Sistema

14.3.1 Control: Software Operativo

14.3.2 Control: Protección de los Datos de Prueba del Sistema

14.3.3 Control: Cambios a Datos Operativos

14.3.4 Control: Acceso a las Bibliotecas de Programas fuentes

14.4 Categoría: Seguridad de los Procesos de Desarrollo y Soporte

14.4.1 Control: Procedimiento de Control de Cambios

14.4.2 Control: Revisión Técnica de los Cambios en el sistema Operativo

14.4.3 Control: Restricción del Cambio de Paquetes de Software

14.4.4 Control: Canales Ocultos y Código Malicioso

14.4.5 Control: Desarrollo Externo de Software

14.5 Categoría: Gestión de vulnerabilidades técnicas

14.5.1 Control: Vulnerabilidades técnicas

15. Cláusula: Relaciones con Proveedores

15.1 Categoría: Seguridad de la información en las relaciones con el proveedor

15.1.1 Control: Política de seguridad de la información para las relaciones con el proveedor

15.1.2 Control: Abordar la seguridad dentro de los acuerdos del proveedor

15.1.3 Control: Cadena de suministro de tecnologías de la información y comunicaciones

15.2 Categoría: Administración de prestación de servicios de proveedores

15.2.1 Control: Supervisión y Revisión de los servicios del proveedor

15.2.2 Control: Gestión de cambios a los servicios del proveedor

16. Cláusula: Gestión de Incidentes de Seguridad

16.1 Categoría: Informe de los eventos y debilidades de la seguridad de la información

16.1.1 Control: Reporte de los eventos de la seguridad de información

16.1.2 Control: Reporte de las debilidades de la seguridad

16.1.3 Control: Comunicación de Anomalías del Software

16.2 Categoría: Gestión de los Incidentes y mejoras de la seguridad de la información

16.2.1 Control: Responsabilidades y procedimientos

16.2.2 Control: Aprendiendo a partir de los incidentes de la seguridad de la información

16.2.3 Control: Procesos Disciplinarios

17. Cláusula: Gestión de la Continuidad

17.1 Categoría: Gestión de continuidad del Organismo

17.1.1 Control: Proceso de Administración de la continuidad del Organismo

17.1.2 Control: Continuidad de las Actividades y Análisis de los impactos

17.1.3 Control: Elaboración e implementación de los planes de continuidad de las Actividades del Organismo

17.1.4 Control: Marco para la Planificación de la Continuidad de las Actividades del Organismo

17.1.5 Control: Ensayo, Mantenimiento y Reevaluación de los Planes de continuidad del Organismo

17.2 Categoría: Redundancias

17.2.1 Control: Disponibilidad de las instalaciones de procesamiento de la información

18. Cláusula: Cumplimiento

18.1 Categoría: Cumplimiento de Requisitos Legales

18.1.1 Control: Identificación de la Legislación Aplicable

18.1.2 Control: Derechos de Propiedad Intelectual

18.1.3 Control: Protección de los Registros del Organismo

18.1.4 Control: Protección de Datos y Privacidad de la Información Personal

18.1.5 Control: Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información

18.1.6 Control: Regulación de Controles para el Uso de Criptografía

18.1.7 Control: Recolección de Evidencia

18.1.8 Control: Delitos Informáticos

18.2 Categoría: Revisiones de la Política de Seguridad y la Compatibilidad Técnica

18.2.1 Control: Cumplimiento de la Política de Seguridad

18.2.2 Control: Verificación de la Compatibilidad Técnica

18.3 Categoría: Consideraciones de Auditorías de Sistemas

18.3.1 Controles de Auditoría de Sistemas

18.3.2 Control: Protección de los Elementos Utilizados por la Auditoría de Sistemas

18.3.3 Control: Sanciones Previstas por Incumplimiento

1. Introducción

En diciembre de 2004, la DA N° 669/2004 de la Jefatura de Gabinete de Ministros estableció la obligatoriedad para los organismos del Sector Público Nacional (comprendidos en los incisos a) y c) del artículo 8° de la Ley N° 24.156 y sus modificatorias) de:

• Dictar una política de Seguridad de la Información conforme la Política de Seguridad Modelo, o adecuar sus Políticas de Seguridad conforme al Modelo aprobado.

• Conformar un Comité de Seguridad en la Información.

• Designar un coordinador del Comité de Seguridad de la Información.

• Establecer las funciones del Comité de Seguridad de la Información.

En 2005 mediante la Disposición N° 6/2005 de la Oficina Nacional de Tecnologías de Información se aprueba la primera “Política de Seguridad de la Información Modelo” y en mayo del 2014 se procedió a realizar la actualización de aquel Modelo, en base a las actualizaciones sufridas por la norma ISO/IEC 27002 versión 2013 y la incorporación de temas como los que se mencionan a continuación:

Los aspectos clave de esta actualización son:

Fundamentales

• Compromiso y apoyo de la dirección de la organización.

• Definición clara de un alcance apropiado.

• Concientización y formación del personal.

• Evaluación de riesgos exhaustiva y adecuada a la organización.

• Compromiso de mejora continua.

• Establecimiento de políticas y normas.

• Organización y comunicación.

• Actualización de controles.

• Inclusión de la cláusula o dominio:

• Criptografía

• Gestión de Proveedores

• Seguridad en las Operaciones

Factores críticos de éxito

• La concientización del empleado por la seguridad. Principal objetivo a conseguir.

• Realización de comités de dirección con descubrimiento continuo de no conformidades o acciones de mejora.

• Creación de un sistema de gestión de incidentes que recoja notificaciones continuas por parte de los usuarios (los incidentes de seguridad deben ser reportados y analizados).

• La seguridad absoluta no existe, se trata de reducir el riesgo a niveles asumibles.

• La seguridad no es un producto, es un proceso.

• La seguridad no es un proyecto, es una actividad continua y el programa de protección requiere el soporte de la organización para tener éxito.

• La seguridad debe ser inherente a los procesos de información y de la organización.

Riesgos

• Temor ante el cambio: resistencia de las personas.

• Discrepancias en los comités de dirección.

• Delegación de todas las responsabilidades en departamentos técnicos.

• No asumir que la seguridad de la información es inherente a los procesos de la organización.

• Planes de formación y concientización inadecuados.

• Definición poco clara del alcance.

• Exceso de medidas técnicas en detrimento de la formación, concientización y medidas de tipo organizativo.

• Falta de comunicación de los progresos al personal de la organización.

Se hace saber que queda expresamente prohibido el uso para fines comerciales del presente documento. Asimismo, las personas autorizadas para usar la "Política Modelo" podrán copiarla, modificarla y reproducirla únicamente para aquellos fines a los cuales está destinada.

El presente modelo podrá sufrir modificaciones futuras, de acuerdo a las novedades que se registren en la materia que trata, las cuales serán debidamente aprobadas y comunicadas.

1.1 Alcance

La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico del Organismo.

Debe ser conocida y cumplida por toda la planta de personal del Organismo, tanto se trate de funcionarios políticos como técnicos, y sea cual fuere su nivel jerárquico y su situación de revista.

1.2 ¿Qué es seguridad de la información?

La información es un activo que, como otros activos importantes, es esencial y en consecuencia necesita ser protegido adecuadamente.

La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida.

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo de la operación y la operación normal del organismo.

La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del organismo.

1.3 ¿Por qué es necesario?

La información y los procesos, sistemas y redes de apoyo son activos importantes. Definir, lograr, mantener y mejorar la seguridad de la información puede ser esencial para mantener una eficacia en la operación de las actividades del organismo, observancia legal e imagen.

Las organizaciones y sus sistemas y redes de información enfrentan amenazas de seguridad de un amplio rango de fuentes; incluyendo fraude por computadora, espionaje, sabotaje, vandalismo, fuego o inundación. Las causas de daño como código malicioso, pirateo computarizado o ataques de denegación servicio se hacen cada vez más comunes, más ambiciosas y cada vez más sofisticadas.

La seguridad de la información es importante tanto para negocios del sector público como privado, y para proteger las infraestructuras críticas. En ambos sectores, la seguridad de la información funcionará como un facilitador; por ejemplo para lograr e-gobierno o e-negocio, para evitar o reducir los riesgos relevantes, La interconexión de redes públicas y privadas y el intercambio de fuentes de información incrementan la dificultad de lograr un control del acceso. La tendencia a la computación distribuida también ha debilitado la efectividad de un control central y especializado.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que se puede lograr a través de medios técnicos es limitada, y debiera ser apoyada por la gestión y los procedimientos adecuados. Identificar qué controles establecer requiere de un planeamiento cuidadoso y prestar atención a los detalles. La gestión de la seguridad de la información requiere, como mínimo, la participación de los diferentes grupos de interés, proveedores, terceros, clientes u otros grupos externos. También se puede requerir asesoría especializada de organizaciones externas.

1.4 Requerimientos de seguridad

Todo comienza con identificar los requerimientos de seguridad. Existen tres fuentes principales de requerimientos de seguridad, Una fuente se deriva de evaluar los riesgos para la organización, tomando en cuenta la estrategia general y los objetivos del organismo.

A través de la evaluación del riesgo, se identifican las amenazas para los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se calcula el impacto potencial.

Otra fuente son los requerimientos legales, reguladores, estatutarios y contractuales que tienen que satisfacer una organización, sus socios comerciales, contratistas y proveedores de servicio; y su ambiente sociocultural.

Otra fuente es el conjunto particular de principios, objetivos y requerimientos funcionales para el procesamiento de la información que una organización ha desarrollado para sostener sus operaciones.

1.5 Evaluación de los riesgos de seguridad

Los requerimientos de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. El gasto en controles debiera ser equilibrado con el daño operacional probable resultado de fallas en la seguridad.

Los resultados de la evaluación del riesgo ayudarán a guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de seguridad de la información, e implementar los controles seleccionados para protegerse contra esos riesgos.

La evaluación del riesgo se debiera repetir periódicamente para tratar cualquier cambio que podría influir en los resultados de la evaluación del riesgo.

Se puede encontrar más información de la evaluación de los riesgos de seguridad en la cláusula 4.1 "Evaluando los riesgos de la seguridad".

1.6 Selección de controles

Una vez que se han identificado los requerimientos y los riesgos de seguridad y se han tomado las decisiones para el tratamiento de los riesgos, se debieran seleccionar los controles apropiados y se debieran implementar para asegurar que los riesgos se reduzcan a un nivel aceptable.

La selección de los controles de seguridad depende de las decisiones organizacionales basadas en el criterio de aceptación del riesgo, opciones de tratamiento del riesgo y el enfoque general para la gestión del riesgo aplicado a la organización, y también debieran estar sujetas a todas las regulaciones y legislación nacionales e internacionales aplicables.

1.7 ¿Cómo empezar?

Se pueden considerar un número de controles como un buen punto de inicio para la implementación de la seguridad de la información. Estos se basan en requerimientos legales esenciales o pueden ser considerados como una práctica común para la seguridad de la información.

Los controles considerados como esenciales para una organización desde el punto de vista legislativo incluyen, dependiendo de la legislación aplicable:

a) protección de datos y privacidad de la información personal,

b) protección de los registros organizacionales,

c) derechos de propiedad intelectual.

Los controles considerados, práctica común para la seguridad de la información, incluyen:

a) documento de la política de seguridad de la información;

b) asignación de responsabilidades de la seguridad de la información;

c) conocimiento, educación y capacitación en seguridad de la información;

d) procesamiento correcto en las aplicaciones;

e) gestión de la vulnerabilidad técnica;

f) gestión de la continuidad operacional;

g) gestión de los incidentes y mejoras de la seguridad de la información.

Estos controles se aplican a la mayoría de las organizaciones y en la mayoría de los escenarios.

Se debiera notar que aunque los controles en esta política son importantes y debieran ser considerados, se debiera determinar la relevancia de cualquier control a la luz de los riesgos específicos que enfrenta la organización. Por lo tanto, aunque el enfoque arriba mencionado es considerado como un buen punto de inicio, no reemplaza la selección de controles basada en la evaluación del riesgo.

1.8 Factores críticos de éxito

La experiencia ha demostrado que los siguientes factores con frecuencia son críticos para una exitosa implementación de la seguridad de la información dentro de una organización:

a) política, objetivos y actividades de seguridad de información que reflejan los objetivos del organismo;

b) un enfoque y marco referencial para implementar, mantener, monitorear y mejorar la seguridad de la información que sea consistente con la cultura organizacional;

c) soporte visible y compromiso de todos los niveles de gestión;

d) un buen entendimiento de los requerimientos de seguridad de la información, evaluación del riesgo y gestión del riesgo;

e) comunicación efectiva de la seguridad de la información con todos los directores, empleados y otras partes para lograr conciencia sobre el tema;

f) distribución de lineamientos sobre la política y los estándares de seguridad de la información para todos los directores, empleados y otras partes involucradas;

g) provisión para el financiamiento de las actividades de gestión de la seguridad de la información;

h) proveer el conocimiento, capacitación y educación apropiados;

i) establecer un proceso de gestión de incidentes de seguridad de la información;

j) implementación de un sistema de medición que se utiliza para evaluar el desempeño en la gestión de la seguridad de la información y retroalimentación de sugerencias para el mejoramiento.

2. Términos y Definiciones

2.1 Seguridad de la Información

La seguridad de la información se entiende como la preservación de las siguientes características:

Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deben considerarse los conceptos de:

Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Sistema de Información. Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología de la Información: Se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Propietario de la Información: Define a la persona responsable de la integridad, confidencialidad y disponibilidad de una cierta información.

2.2 Evaluación de Riesgos

Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.

2.2 Tratamiento de Riesgos

Proceso de selección e implementación de medidas para modificar el riesgo.

2.3 Gestión de Riesgos

Actividades coordinadas para dirigir y controlar una organización en lo que concierne al riesgo.

NOTA. La gestión de riesgos usualmente incluye la evaluación de riesgos, el tratamiento de riesgos, la aceptación de riesgos y la comunicación de riesgos.

2.4 Comité de Seguridad de la Información

El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

2.5 Responsable de Seguridad de la Información

Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.

2.6 Incidente de Seguridad

Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que puede comprometer o compromete la confidencialidad, integridad y/o disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

2.7 Riesgo

Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impacto.

2.8 Amenaza

Una causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización.

2.9 Vulnerabilidad

Una debilidad de un activo o grupo de activos que puede ser aprovechada por una amenaza.

2.10 Control

Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales, las cuales pueden ser de naturaleza administrativa, técnica, de gestión, o legal.

NOTA. Control es también utilizado como sinónimo de salvaguarda o de contramedida.

3. Estructura de la política Modelo

Este modelo que se divide en dos partes, y guarda la siguiente estructura:

• Cuatro capítulos introductorios, con los términos generales y el establecimiento de la Evaluación y el Tratamiento de los riesgos,

• Catorce cláusulas que abarcan los diferentes aspectos o dominios de la seguridad de la información. Se presentan de manera sistemática y consistente.



Cada cláusula contiene un número de categorías o grupo de controles de seguridad principales. Las catorce cláusulas (acompañadas por el número de categorías de seguridad principales incluidas dentro de cada cláusula) son:

- Política de Seguridad (1);

- Organización (2);

- Recursos Humanos (3);

- Gestión de Activos (3);

- Gestión de Accesos (5);

- Criptografía (1);

- Seguridad Física y Ambiental (2);

- Seguridad de las Operaciones (7);

- Seguridad de las Comunicaciones (2);

- Adquisición, Desarrollo y Mantenimiento de Sistemas (5);

- Relaciones con Proveedores (3);

- Gestión de Incidentes de seguridad de la información (2);

- Gestión de la Continuidad (2);

- Cumplimiento (3).

Por último, por cada categoría, se establece un objetivo y contiene uno o más controles a realizar.

A modo de síntesis se enuncia a continuación la estructura de cada cláusula:

- Cláusula o dominio

1. Generalidades

2. Objetivos

3. Alcance

4 Responsabilidades

5. Política

- Categorías

• Objetivo

- Controles

Las catorce cláusulas o dominios son:

- Cláusulas

1. Política de seguridad

2. Organización

3. Recursos humanos

4. Gestión de activos

5. Gestión de Accesos

6. Criptografía

7. Seguridad Física y Ambiental

8. Seguridad de las operaciones

9. Seguridad de las comunicaciones

10. Adquisición, desarrollo y mantenimiento de sistemas

11. Relaciones con Proveedores

12. Gestión de Incidentes de seguridad de la información

13. Gestión de continuidad

14. Cumplimento

4. Evaluación y tratamiento de riesgos

Generalidades

Todo Organismo se encuentra expuesto a riesgos en materia de seguridad de la información. No existe la seguridad completa, por lo que es necesario conocer cuál es el mapa de riesgos al cual se enfrenta el organismo y tomar acciones tendientes a minimizar los posibles efectos negativos de la materialización de dichos riesgos.

Es por ello que resulta imprescindible gestionar los riesgos del Organismo, como pilar fundamental para la gestión de seguridad.

Objetivo

Conocer los riesgos a los que se expone el Organismo en materia de seguridad de la información.

Generar información de utilidad para la toma de decisiones en materia de controles de seguridad.

Alcance

Esta Política se aplica a toda la información administrada en el Organismo, cualquiera sea el soporte en que se encuentre.

Responsabilidad

El Comité de Seguridad de la Información será responsable de que se gestionen los riesgos de seguridad de la información, brindando su apoyo para el desarrollo de dicho proceso y su mantenimiento en el tiempo.

El Responsable de Seguridad de la Información junto con los Titulares de Unidades Organizativas será responsable del desarrollo del proceso de gestión de riesgos de seguridad de la información.

Política

4.1 Evaluación de los riesgos de seguridad

El Organismo evaluará sus riesgos identificándolos, cuantificándolos y priorizándolos en función de los criterios de aceptación de riesgos y de los objetivos de control relevantes para el mismo. Los resultados guiarán y determinarán la apropiada acción de la dirección y las prioridades para gestionar los riesgos de seguridad de la información y para la implementación de controles seleccionados para protegerse contra estos riesgos.

Se debe efectuar la evaluación de riesgos periódicamente, para tratar con los cambios en los requerimientos de seguridad y en las situaciones de riesgo, por ejemplo: cambios producidos en activos, amenazas, vulnerabilidades, impactos, valoración de riesgos. Asimismo, se debe efectuar la evaluación cada vez que ocurran cambios significativos. Es conveniente que estas evaluaciones de riesgos se lleven a cabo de una manera metódica capaz de producir resultados comparables y reproducibles.

El alcance de una evaluación de riesgos puede incluir a todo el Organismo, una parte, un sistema de información particular, componentes específicos de un sistema, o servicios. Resulta recomendable seguir una metodología de evaluación de riesgos para llevar a cabo el proceso.

4.2 Tratamiento de riesgos de seguridad

Antes de considerar el tratamiento de un riesgo, el Organismo debe decidir los criterios para determinar si los riesgos pueden, o no, ser aceptados. Los riesgos pueden ser aceptados si por ejemplo: se evaluó que el riesgo es bajo o que el costo del tratamiento no es económicamente viable para la organización. Tales decisiones deben ser tomadas por las autoridades y debidamente documentadas.

Para cada uno de los riesgos identificados durante la evaluación de riesgos, se necesita tomar una decisión para su tratamiento. Las posibles opciones para el tratamiento de riesgos incluyen:

a) Mitigar los riesgos mediante la aplicación de controles apropiados para reducir los riesgos;

b) Aceptar los riesgos de manera objetiva y consciente, siempre y cuando éstos satisfagan claramente la política y los criterios de aceptación de riesgos del Organismo;

c) Evitar los riesgos, eliminando las acciones que dan origen a la ocurrencia de estos;

d) Transferir los riesgos asociados a otras partes interesadas, por ejemplo: compañías de seguro o proveedores.

Para aquellos riesgos donde la decisión ha sido la mitigación, se buscará reducir los riesgos a un nivel aceptable mediante la implementación de controles, teniendo en cuenta lo siguiente:

a) requerimientos y restricciones de legislaciones y regulaciones nacionales e internacionales;

b) objetivos organizacionales;

c) requerimientos y restricciones operativos;

d) costo de implementación y operación en relación directa a los riesgos reducidos, y proporcionales a los requerimientos y restricciones del Organismo;

e) la necesidad de equilibrar las inversiones en la implementación y operación de los controles contra el daño que podría resultar de las fallas de seguridad.

Los controles a implementar pueden ser seleccionados del contenido de las cláusulas de esta política, o se pueden establecer nuevos controles para satisfacer necesidades específicas del Organismo. Es necesario reconocer que algunos controles pueden no ser aplicables a todo sistema de información o a su ambiente, y podrían no ser aplicables en todos los Organismos.

Se debe recordar que ningún conjunto de controles puede alcanzar la seguridad absoluta. Los controles implementados deben ser evaluados permanentemente para que puedan ser mejorados en eficiencia y efectividad.

5. Cláusula: Política de Seguridad de la Información



Generalidades

La información es un recurso que, como el resto de los activos, tiene valor para el Organismo y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información y de la operación del Organismo, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Organismo.

Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional.

Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades del Organismo y de los titulares de Unidades Organizativas para la difusión, consolidación y cumplimiento de la presente Política.

Objetivo

Proteger los recursos de información del Organismo y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales,

Mantener la Política de Seguridad del Organismo actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Alcance

Esta Política se aplica en todo el ámbito del Organismo, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Responsabilidad

Todos los Directores Nacionales o Generales, Gerentes o equivalentes, titulares de Unidades Organizativas, tanto se trate de autoridades políticas o personal técnico y sea cual fuere su nivel jerárquico son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal del Organismo, cualquiera sea su situación de revista, el área a la cual se encuentre afectada y cualquiera sea el nivel de las tareas que desempeñe.

Las máximas autoridades del Organismo aprueban esta Política y son responsables de la autorización de sus modificaciones.

El Comité de Seguridad de la Información del Organismo,

- procederá a revisar y proponer a la máxima autoridad del Organismo para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información;

- monitoreará cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes;

- tomará conocimiento y supervisará la investigación y monitoreo de los incidentes relativos a la seguridad;

- aprobará las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área[1], así como acordará y aprobará metodologías y procesos específicos relativos a seguridad de la información;

- garantizará que la seguridad sea parte del proceso de planificación de la información; evaluará y coordinará la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios;

- promoverá la difusión y apoyo a la seguridad de la información dentro del Organismo y coordinará el proceso de administración de la continuidad de las actividades del Organismo.

[1] Se refiere a dar curso a las propuestas presentadas por parte de las áreas de acuerdo a sus competencias, elevándolas a la máxima autoridad, a través del Comité de Seguridad, con relación a la seguridad de la información del Organismo. Dichas iniciativas deben ser aprobadas luego por la máxima autoridad del Organismo.

El Coordinador del Comité de Seguridad de la Información será el responsable de:

• coordinar las acciones del Comité de Seguridad de la Información y de

• impulsar la implementación y cumplimiento de la presente Política.

El Responsable de Seguridad de la Información:

• cumplirá funciones relativas a la seguridad de los sistemas de información del Organismo, lo cual incluye: la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política.

Los Propietarios de la información y Propietarios de activos son responsables de:

• clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma,

• documentar y mantener actualizada la clasificación efectuada, y

• definir qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

El Responsable del Área de Recursos Humanos o quien desempeñe esas funciones, cumplirá la función de:

• notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan.

• Asimismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continua en materia de seguridad.

El Responsable del Área Informática cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología del Organismo. Por otra parte tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

El Responsable del Área Legal o Jurídica verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación del Organismo con los empleados y, en caso de existir, con los terceros. Asimismo, asesorará en materia legal al Organismo, en lo que se refiere a la seguridad de la información.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

La Unidad de Auditoría Interna, o en su defecto quien sea propuesto por el Comité de Seguridad de la Información es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan (Ver Cláusula 18: Cumplimiento),

Política

5.1 Categoría: Política de Seguridad de la información

Objetivo

Proporcionar a la Dirección Superior la dirección y soporte para la seguridad de la información en concordancia con los requerimientos y las leyes y regulaciones relevantes. La gerencia debe establecer claramente la dirección de la política en línea con los objetivos.

5.1.1 Control: Documento de la política de seguridad de la información

El documento de la política debe ser aprobado por el Comité de Seguridad, publicado y comunicado a todos los empleados y las partes externas relevantes.

Esta Política se conforma de una serie de pautas sobre aspectos específicos de la Seguridad de la información, que incluyen los siguientes tópicos:

Organización de la Seguridad

Orientado a administrar la seguridad de la información dentro del Organismo y establecer un marco gerencial para controlar su implementación.

Gestión de Activos

Destinado a mantener una adecuada protección de los activos del Organismo.

Recursos Humanos

Orientado a reducir los riesgos de error humano, comisión de ilícitos contra el Organismo o uso inadecuado de instalaciones.

Física y Ambiental

Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información del Organismo.

Gestión de las Comunicaciones y las Operaciones

Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.

Gestión de Accesos

Orientado a controlar el acceso lógico a la información.

Adquisición. Desarrollo y Mantenimiento de los Sistemas

Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su adquisición, desarrollo y/o implementación y durante su mantenimiento.

Gestión de Incidentes de seguridad

Orientado a administrar todos los eventos que atenten contra la confidencialidad, integridad y disponibilidad de la información y los activos tecnológicos

Gestión de Continuidad

Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.

Cumplimiento

Destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

A fin de asegurar la implementación de las medidas de seguridad comprendidas en esta Política, el Organismo identificará los recursos necesarios e indicará formalmente las partidas presupuestarias correspondientes, como anexo a la presente Política. Lo expresado anteriormente no implicará necesariamente la asignación de partidas presupuestarias adicionales.

La máxima autoridad del Organismo aprobará formalmente la Política y la comunicará a todos los empleados, mediante el Responsable del Area de Recursos Humanos y terceras partes relevantes.

5.1.2 Control: Revisión de la política de seguridad de la información

La política de seguridad de la información debe tener un dueño, responsable de las actividades de desarrollo, evaluación y revisión de la política.

La actividad de revisión debe incluir las oportunidades de mejoras, en respuesta a los cambios, entre otros: organizacionales, normativos, legales, de terceros, tecnológicos.

Las mejoras tenidas en cuenta deben quedar registradas y tener las aprobaciones de los responsables.

El Comité de Seguridad de la Información debe revisarla a intervalos planeados y prever el tratamiento de caso de los cambios no planeados, a efectos de mantener actualizada la política.

Asimismo efectuará toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como ser, cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, etc.

6. Cláusula: Organización



Generalidades

La presente Política de Seguridad establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades del Organismo.

Por ello, se definirá formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades.

Asimismo, se contemplará la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad de la información.

Por otro lado debe tenerse en cuenta que ciertas actividades del Organismo pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

Objetivo

Administrar la seguridad de la información dentro del Organismo y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

Fomentar la consulta y cooperación con Organismos especializados para la obtención de asesoría en materia de seguridad de la información.

Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información del Organismo.

Alcance

Esta Política se aplica a todos los recursos del Organismo y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

Responsabilidad

El Coordinador del Comité de Seguridad de la Información será el responsable de impulsar la implementación de la presente Política.

El Comité de Seguridad de la Información tendrá a cargo el mantenimiento y la presentación para la aprobación de la presente Política, ante la máxima autoridad del organismo, el seguimiento

de acuerdo a las incumbencias propias de cada área de las actividades relativas a la seguridad de la información (análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles, administración de la continuidad, impulsión de procesos de concientización, etc.) y la proposición de asignación de funciones.

El Responsable de Seguridad de la información asistirá al personal del Organismo en materia de seguridad de la información y coordinará la interacción con Organismos especializados. Asimismo, junto con los propietarios de la información, analizará el riesgo de los accesos de terceros a la información del Organismo y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

Los Responsables de las Unidades Organizativas cumplirán la función de autorizar la incorporación de nuevos recursos de procesamiento de información a las áreas de su incumbencia.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información será responsable de realizar revisiones independientes sobre la vigencia y el cumplimiento de la presente Política.

El Responsable del Área de Administración cumplirá la función de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas relacionadas.

El Responsable del Área Jurídica participará en dicha tarea.

Asimismo, notificará a los proveedores sobre las modificaciones que se efectúen a la Política de Seguridad de la Información del Organismo.

Política

6.1 Categoría: Organización interna

Objetivo

Manejar la seguridad de la información dentro del organismo.

Se debe establecer un marco referencial gerencial o política, para iniciar y controlar la implementación de la seguridad de la información dentro del organismo.

La Dirección debe aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implementación de la seguridad en todo el organismo.

6.1.1 Control: Compromiso de la dirección con la seguridad de la información

La dirección debe apoyar la seguridad de la información a través de una dirección clara, mostrando compromiso, asignando roles y reconociendo responsabilidades explícitas.

Debe formular, revisar y aprobar la política de seguridad de la información, como asimismo revisar los beneficios de la implementación de la misma.

La seguridad de la información es una responsabilidad del Organismo compartida por todas las Autoridades políticas y Directores Nacionales o Generales, Gerentes o equivalentes, por lo cual se crea el Comité de Seguridad de la Información, integrado por representantes de todos los Directores mencionados, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad de la información. El mismo contará con un Coordinador, quien cumplirá la función de impulsar la implementación de la presente Política.

Conformación del Comité de Seguridad de la Información

Área/Dirección	Representante

Este Comité tendrá entre sus funciones:

a) Revisar y proponer a la máxima autoridad del Organismo para su aprobación, la Política y las funciones generales en materia de seguridad de la información.

b) Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

c) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.

d) Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área[2].

e) Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.

f) Garantizar que la seguridad sea parte del proceso de planificación informática del Organismo.

g) Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.

h) Promover la difusión y apoyo a la seguridad de la información dentro del Organismo.

i) Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información del Organismo frente a interrupciones imprevistas.

El…………………..(Subsecretario de Coordinación o equivalente en cada área ministerial o Secretaría de la Presidencia de la Nación o el funcionario designado por las máximas autoridades en cada Organismo descentralizado - Indicar cargo) coordinará las actividades del Comité de Seguridad de la Información.

[2] Se refiere a dar curso a las propuestas presentadas por parte de las áreas de acuerdo a sus competencias, elevándolas a la máxima autoridad, a través del Comité de Seguridad, con relación a la seguridad de la información del Organismo. Dichas iniciativas deben ser aprobadas luego por la máxima autoridad del Organismo.

6.1.2 Control: Coordinación de la seguridad de la información

Típicamente, la coordinación de la seguridad de la información debiera involucrar la cooperación y colaboración de los Directores Nacionales o Generales, Gerentes o equivalentes, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad, y capacidades especializadas en áreas como seguros, temas legales, recursos humanos, TI o gestión del riesgo. Esta actividad debiera:

a) asegurar que las actividades de seguridad sean ejecutadas en conformidad con la política de seguridad de la información;

b) identificar cómo manejar las no-conformidades;

c) aprobar las metodologías y procesos para la seguridad de la información; por ejemplo, la evaluación del riesgo y la clasificación de la información;

d) identificar cambios significativos en las amenazas y la exposición de la información y los medios de procesamiento de la información ante amenazas;

e) evaluar la idoneidad y coordinar la implementación de los controles de la seguridad de información;

f) promover de manera efectiva la educación, capacitación y conocimiento de la seguridad de la información a través de toda la organización;

g) evaluar la información recibida del monitoreo y revisar los incidentes de seguridad de la información, y recomendar las acciones apropiadas en respuesta a los incidentes de seguridad de información identificados.

6.1.3 Control: Asignación de responsabilidades de la seguridad de la información

La asignación de responsabilidades de la seguridad de la información debe ejecutarse en forma alineada a la política de seguridad de la información (ver cláusula 5 política de seguridad de la información).

El……………………………(Indicar la máxima autoridad del Organismo), asigna las funciones relativas a la Seguridad Informática del Organismo a………………………(indicar cargo), en adelante el "Responsable de Seguridad de la Información", quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información del Organismo, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática tratados en la presente Política.

El Comité de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación la definición y asignación de las responsabilidades que surjan del presente Modelo.

A continuación se detallan los procesos de seguridad, indicándose en cada caso el/los responsable/s del cumplimiento de los aspectos de esta Política aplicables a cada caso:

Proceso	Responsable
Seguridad del Personal	………..
Seguridad Física y Ambiental	………..
Seguridad en las Comunicaciones y las Operaciones	………..
Control de Accesos	………..
Seguridad en el Desarrollo y Mantenimiento de Sistemas	………..
Planificación de la Continuidad Operativa	………..
………..	………..

De igual forma, seguidamente se detallan los propietarios de la información, quienes serán los Responsables de las Unidades Organizativas a cargo del manejo de la misma:

Información	Propietario	Recursos asociados	Procesos involucrados	Administrador
Contable	………………	Sistemas de información, equipamiento, bases de datos, comunicaciones, …………….	…………….	………………
Presupuesto o Inventario ………………	………………	…………….	…………….	………………

Cabe aclarar que, si bien los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservarán la responsabilidad del cumplimiento de las mismas. La

delegación de la administración por parte de los propietarios de la información será documentada por los mismos y proporcionada al Responsable de Seguridad de la Información.

6.1.4 Control: Autorización para Instalaciones de Procesamiento de Información

Los nuevos recursos de procesamiento de información serán autorizados por los Responsables de las Unidades Organizativas involucradas, considerando su propósito y uso, conjuntamente con el Responsable de Seguridad de la Información, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad pertinentes.

Las siguientes guías deben ser consideradas para el proceso de autorización:

a) Cumplir con los niveles de aprobación vigentes en la organización, incluso el responsable del ambiente de seguridad de la información, asegurando el cumplimiento de las políticas y requerimientos.

b) Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas del Organismo.

c) El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso será evaluado en cada caso por el Responsable de Seguridad de la Información y debe ser autorizado por el Responsable del Área Informática y por el Director Nacional (General, Gerente o equivalente en el Organismo) responsable del área al que se destinen los recursos.

6.1.5 Control: Acuerdos de confidencialidad

Se definirán, implementarán y revisarán regularmente los acuerdos de confidencialidad o de no divulgación para la protección de la información del Organismo. Dichos acuerdos deben responder a los requerimientos de confidencialidad o no divulgación del Organismo, los cuales serán revisados periódicamente. Asimismo, deben cumplir con toda legislación o normativa que alcance al Organismo en materia de confidencialidad de la información.

Dichos acuerdos deben celebrarse tanto con el personal del organismo como con aquellos terceros que se relacionen de alguna manera con su información.

6.1.6 Control: Contacto con otros organismos

A efectos de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad, se mantendrán contactos con los siguientes Organismos especializados en temas relativos a la seguridad informática:

Oficina Nacional de Tecnologías de Información (ONTI) dependiente de la Subsecretaría de Tecnologías de Gestión de la Secretaría de Gabinete y Coordinación Administrativa de la Jefatura de Gabinete de Ministros:

Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC). Es una unidad de respuesta ante incidentes en redes y sistemas, que centraliza y coordina los esfuerzos ante los incidentes de seguridad que afecten a los recursos informáticos del Sector Público.

Dirección Nacional de Protección de Datos Personales dependiente del Ministerio de Justicia y Derechos Humanos. En los intercambios de información de seguridad, no se divulgará información sensible (de acuerdo a lo definido en la normativa vigente, ej.: Ley 25.326) o confidencial perteneciente al Organismo a personas no autorizadas.

El intercambio de información confidencial para fines de asesoramiento o de transmisión de experiencias, sólo se permite cuando se haya firmado un Acuerdo de Confidencialidad previo o con aquellas Organizaciones especializadas en temas relativos a la seguridad de la Información cuyo personal está obligado a mantener la confidencialidad de los temas que trata.

6.1.7 Control: Contacto con grupos de interés especial

El Responsable de Seguridad de la información será el encargado de coordinar los conocimientos y las experiencias disponibles en el Organismo a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Éste podrá obtener asesoramiento de otros Organismos. Con el objeto de optimizar su gestión, se habilitará al Responsable de Seguridad de la Información el contacto con las Unidades Organizativas de todas las Áreas del Organismo.

Debe considerar ser miembro de grupos de interés especial para:

a) Adquirir nuevos conocimientos acerca de las mejores prácticas y estar actualizado;

b) Asegurar que la concientización acerca de la seguridad de la información esté actualizada y completa;

c) Recibir alertas tempranas, avisos y recomendaciones ante ataques y vulnerabilidades;

d) Proporcionar vínculos adecuados durante el tratamiento de los incidentes de seguridad de la información.

6.1.8 Control: Revisión independiente de la seguridad de la información

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la información realizará revisiones independientes sobre la vigencia, implementación y gestión de la Política de Seguridad de la Información, a efectos de garantizar que las prácticas del Organismo reflejan adecuadamente sus disposiciones.

Estas revisiones deben incluir las oportunidades de evaluación de mejoras y las necesidades de cambios de enfoque en la seguridad, incluyendo políticas y objetivos de control.

Se deben registrar y reportar todas estas actividades.

6.2 Categoría: Dispositivos móviles y trabajo remoto

Objetivo

Asegurar la seguridad de la información cuando se utiliza medios de computación y teletrabajo móviles.

La protección requerida se debe conmensurar con los riesgos que causan estas maneras de trabajo específicas. Cuando se utiliza computación móvil, se deben considerar los riesgos de trabajar en un ambiente desprotegido y se debiera aplicar la protección apropiada. En el caso del tele-trabajo, la organización debe aplicar protección al lugar del tele-trabajo y asegurar que se establezcan los arreglos adecuados para esta manera de trabajar.

6.2.1 Control: Dispositivos Móviles

Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información ni la infraestructura del Organismo.

Se debe tener en cuenta en este sentido, cualquier dispositivo móvil y/o removible, incluyendo: Notebooks, Laptop o PDA (Asistente Personal Digital), Teléfonos Celulares y sus tarjetas de memoria, Dispositivos de Almacenamiento removibles, tales como CDs, DVDs, Disquetes, Tapes, y cualquier dispositivo de almacenamiento de conexión USB, Tarjetas de identificación personal (control de acceso), dispositivos criptográficos, cámaras digitales, etc.

Esta lista no es taxativa, ya que deben incluirse todos los dispositivos que pudieran contener información confidencial del Organismo y por lo tanto, ser pasibles de sufrir un incidente en el que se comprometa la seguridad del mismo.

Se desarrollarán procedimientos adecuados para estos dispositivos, que abarquen los siguientes conceptos:

a) La protección física necesaria.

b) El acceso seguro a los dispositivos.

c) La utilización segura de los dispositivos en lugares públicos.

d) El acceso a los sistemas de información y servicios del Organismo a través de dichos dispositivos.

e) Las técnicas criptográficas a utilizar para la transmisión de información clasificada.

f) Los mecanismos de resguardo de la información contenida en los dispositivos.

g) La protección contra software malicioso.

La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de pérdida, robo o hurto. En consecuencia debe entrenarse especialmente al personal que los utilice. Se desarrollarán normas y procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles, que contemplarán las siguientes recomendaciones:

a) Permanecer siempre cerca del dispositivo.

b) No dejar desatendidos los equipos.

c) No llamar la atención acerca de portar un equipo valioso.

d) No poner identificaciones del Organismo en el dispositivo, salvo los estrictamente necesarios.

e) No poner datos de contacto técnico en el dispositivo.

f) Mantener cifrada la información clasificada.

Por otra parte, se confeccionarán procedimientos que permitan al poseedor del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información del Organismo, los que incluirán:

a) Revocación de las credenciales afectadas

b) Notificación a grupos de Trabajo donde potencialmente se pudieran haber comprometido recursos.

6.2.2 Control: Trabajo Remoto

El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo al Organismo.

El trabajo remoto sólo será autorizado por el Responsable de la Unidad Organizativa, o superior jerárquico correspondiente, a la cual pertenezca el usuario solicitante, conjuntamente con el Responsable de Seguridad de la Información, cuando se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes.

Estos casos serán de excepción y serán contemplados en situaciones que justifiquen la imposibilidad de otra forma de acceso y la urgencia, tales como horarios del Organismo, solicitud de las autoridades, etc.

Para ello, se establecerán normas y procedimientos para el trabajo remoto, que consideren los siguientes aspectos:

a) La seguridad física existente en el sitio de trabajo remoto, tomando en cuenta la seguridad física del edificio y del ambiente local.

b) El ambiente de trabajo remoto propuesto.

c) Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos del Organismo, la sensibilidad de la información a la que se accederá y que pasará a través del vínculo de comunicación y la sensibilidad del sistema interno.

d) La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo, familia y amigos.

e) Evitar la instalación / desinstalación de software no autorizado por el Organismo.

Los controles y disposiciones comprenden:

a) Proveer de mobiliario para almacenamiento y equipamiento adecuado para las actividades de trabajo remoto.

b) Definir el trabajo permitido, el horario de trabajo, la clasificación de la información que se puede almacenar en el equipo remoto desde el cual se accede a la red del Organismo y los sistemas internos y servicio a los cuales el trabajador remoto está autorizado a acceder.

c) Proveer de un adecuado equipo de comunicación, con inclusión de métodos para asegurar el acceso remoto.

d) Incluir seguridad física.

e) Definir reglas y orientación respecto del acceso de terceros al equipamiento e información.

f) Proveer el hardware y el soporte y mantenimiento del software.

g) Definir los procedimientos de backup y de continuidad de las operaciones.

h) Efectuar auditoría y monitoreo de la seguridad.

i) Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.

j) Asegurar el reintegro del equipamiento en las mismas condiciones en que fue entregado, en el caso en que cese la necesidad de trabajar en forma remota.

Se implementarán procesos de auditoría específicos para los casos de accesos remotos, que serán revisados regularmente. Se llevará un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.

7. Cláusula: Recursos Humanos



Generalidades

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de revista, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

La implementación de la Política de Seguridad de la Información tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos y evitar eventuales replicaciones. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes, que no pudieron prevenirlo, y evitarlo en el futuro.

Objetivo

Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos de confidencialidad a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad del Organismo en el transcurso de sus tareas normales.

Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.

Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Alcance

Esta Política se aplica a todo el personal del Organismo, cualquiera sea su situación de revista, y al personal externo que efectúe tareas dentro del ámbito del Organismo.

Responsabilidad

El Responsable del Área de Recursos Humanos incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente Política.

El Responsable del Área Jurídica participará en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en el organismo, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente Política y en el tratamiento de incidentes de seguridad que requieran de su intervención.

Política

7.1 Categoría: Antes del empleo

Objetivo

Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios.

Las responsabilidades de seguridad deben ser tratadas antes del empleo en las definiciones de trabajo adecuadas y en los términos y condiciones del empleo.

7.1.1 Control: Funciones y responsabilidades

Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo.

Éstas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

Se definirán y comunicarán claramente los roles y responsabilidades de seguridad a los candidatos para el puesto de trabajo durante el proceso de preselección.

7.1.2 Control: Investigación de antecedentes

Se llevarán a cabo controles de verificación del personal en el momento en que se solicita el puesto. Estos controles incluirán todos los aspectos que indiquen las normas que a tal efecto alcanzan al Organismo.

Los chequeos de verificación deben incluir:

a) Disponibilidad de referencias de carácter satisfactorias

b) Chequeo del currículum vitae del postulante

c) Confirmación de títulos académicos y profesionales mencionados por el postulante

d) Acreditación de su identidad

7.1.3 Control: Términos y condiciones de contratación

Como parte de sus términos y condiciones iniciales de empleo, los empleados, cualquiera sea su situación de revista, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información del Organismo. La copia firmada del Compromiso debe ser retenida en forma segura por el Área de Recursos Humanos u otra competente.

Asimismo, mediante el Compromiso de Confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

Se desarrollará un procedimiento para la suscripción del Compromiso de Confidencialidad donde se incluirán aspectos sobre:

Suscripción inicial del Compromiso por parte de la totalidad del personal. Revisión del contenido del Compromiso cada ….. (indicar período no mayor al año).

Método de re-suscripción en caso de modificación del texto del Compromiso.

Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información.

Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede del Organismo y del horario normal de trabajo.

Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de empleo.

7.2 Categoría: Durante el empleo

Objetivo

Asegurar que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.

Se deben definir las responsabilidades de la gerencia para asegurar que se aplique la seguridad a lo largo de todo el tiempo del empleo de la persona dentro del Organismo.

7.2.1 Control: Responsabilidad de la dirección

La dirección solicitará a los empleados, contratistas y usuarios de terceras partes que apliquen la seguridad en concordancia con las políticas y procedimientos establecidos por la organización, cumpliendo con lo siguiente:

a) estar adecuadamente informados de sus roles y responsabilidades de seguridad de la información antes de que se les otorgue el acceso a información sensible o a los sistemas de información;

b) ser provistos de guías para establecer las expectativas de seguridad de su rol dentro del Organismo;

c) ser motivados para cumplir con las políticas de seguridad del Organismo;

d) alcancen un nivel de conciencia sobre la seguridad acorde con sus roles y responsabilidades dentro del Organismo;

e) cumplir con las condiciones y términos del empleo, los cuales incluyen las políticas de seguridad de la información del Organismo y métodos adecuados de trabajo;

f) mantenerse con las habilidades y calificaciones adecuadas.

Si los empleados, contratistas y usuarios no son conscientes de sus responsabilidades de seguridad, ellos pueden causar daños considerables al organismo. Un personal motivado tiene más probabilidades de ser más confiable y causar menos incidentes de seguridad de la información.

7.2.2 Control: Concientización, formación y capacitación en seguridad de la información

Todos los empleados del Organismo y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en el organismo, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos del Organismo. Esto com-

prende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

El Responsable del Área de Recursos Humanos será el encargado de coordinar las acciones de capacitación que surjan de la presente Política.

Cada …………….. (Indicar periodicidad no mayor a un año) se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento.

Las siguientes áreas serán encargadas de generar el material de capacitación

Áreas Responsables del Material de Capacitación

…………………………..

…………………………..

Adicionalmente, las áreas responsables de generar el material de capacitación dispondrán de información sobre seguridad de la Información para la Administración Pública Nacional en la Coordinación de Emergencias en Redes Teleinformáticas para complementar los materiales por ellas generados.

El personal que ingrese al Organismo recibirá el material, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

Por otra parte, se arbitrarán los medios técnicos necesarios para comunicar a todo el personal, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.

7.2.3 Control: Proceso disciplinario

Se seguirá el proceso disciplinario formal contemplado en las normas estatutarias, escalafonarias y convencionales que rigen al personal de la Administración Pública Nacional, para los empleados que violen la Política, Normas y Procedimientos de Seguridad del Organismo.

El proceso disciplinario también se puede utilizar como un elemento disuasivo para evitar que los empleados, contratistas y terceros que violen las políticas y procedimientos de la seguridad del organismo y cualquier otro incumplimiento de la seguridad.

7.3 Categoría: Cese del empleo o cambio de puesto de trabajo

Objetivo

Asegurar que los usuarios empleados, contratistas y terceras personas salgan del Organismo o cambien de empleo de una manera ordenada.

Se deben establecer las responsabilidades para asegurar que la salida del Organismo del usuario empleado, contratista o tercera persona sea manejada y se complete la devolución de todo el equipo y se eliminen todos los derechos de acceso.

7.3.1 Control: Responsabilidad del cese o cambio

Las responsabilidades para realizar la desvinculación o cambio de puesto deben ser claramente definidas y asignadas, incluyendo requerimientos de seguridad y responsabilidades legales a posteriori y, cuando sea apropiado, las responsabilidades contenidas dentro de cualquier acuerdo de confidencialidad, y los términos y condiciones de empleo con continuidad por un período definido de tiempo luego de la finalización del trabajo del empleado, contratista o usuario de tercera parte.

Puede ser necesario informar a los empleados, contratistas y terceros de los cambios en el personal y los acuerdos de operación.

7.3.2 Control: Devolución de activos

Todos los empleados, contratistas y usuarios de terceras partes deben devolver todos los activos de la organización en su poder (software, documentos corporativos, equipamiento, dispositivos de computación móviles, tarjetas de crédito, tarjetas de ingreso, etc.) tras la terminación de su empleo, contrato, o acuerdo.

En los casos donde el empleado, contratista y usuarios tengan conocimiento que es importante para las operaciones actuales, esa información debe ser documentada y transferida al organismo.

7.3.3 Control: Retiro de los derechos de acceso

Se revisarán los derechos de acceso de un individuo a los activos asociados con los sistemas y servicios de información tras la desvinculación. Esto determinará si es necesario remover los derechos de acceso.

Con el cambio de un empleo deben removerse todos los derechos de acceso que no fueron aprobados para el nuevo empleo, comprendiendo esto accesos lógicos y físicos, llaves, tarjetas de identificación, instalaciones de procesamiento de la información, suscripciones, y remoción de cualquier documentación que lo identifique como un miembro corriente del Organismo.

Si un empleado, contratista o usuario de tercera parte que se está desvinculando tiene conocimiento de contraseñas para cuentas que permanecen activas, éstas deben ser cambiadas tras la finalización o cambio de empleo, contrato o acuerdo.

Se evaluará la reducción o eliminación de los derechos de acceso a los activos de la información y a las instalaciones de procesamiento de la información antes de que el empleo termine o cambie, dependiendo de factores de riesgos, tales como:

a) si la terminación o cambio es iniciado por el empleado, contratista o usuario de tercera parte, o por la gestión y la razón de la finalización;

b) las responsabilidades actuales del empleado, contratista o cualquier otro usuario;

c) el valor de los activos accesibles actualmente.

8. Cláusula: Gestión de Activos



Generalidades

El Organismo debe tener un conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

• Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.

• Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo y publicación de contenidos, utilitarios, etc.

• Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos, switches de datos, etc.), medios magnéticos (cintas, discos, dispositivos móviles de almacenamiento de datos —pen drives, discos externos, etc.—), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado, controles automatizados de acceso, etc.), mobiliario, lugares de emplazamiento, etc.

• Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Generalmente, la información deja de ser sensible o crítica después de un cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en gastos adicionales innecesarios para el Organismo.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información.

Por último, la información puede pasar a ser obsoleta y por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

Objetivo

• Garantizar que los activos de información reciban un apropiado nivel de protección.

• Clasificar la información para señalar su sensibilidad y criticidad.

• Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Alcance

Esta Política se aplica a toda la información administrada en el Organismo, cualquiera sea el soporte en que se encuentre.

Responsabilidad

Los Propietarios de los Activos son los encargados de clasificarlos de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, de definir las funciones que deben tener permisos de acceso a los activos y son responsables de mantener los controles adecuados para garantizar su seguridad.

El Responsable de Seguridad de la Información es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la presente Política.

Política

8.1 Categoría: Responsabilidad sobre los activos

Objetivo

Todos los activos deben ser inventariados y contar con un propietario nombrado.

Los propietarios deben identificar todos los activos y se debiera asignar la responsabilidad por el mantenimiento de los controles apropiados. La implementación de controles específicos puede ser delegada por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección apropiada de los activos.

8.1.1 Control: Inventario de activos

Se identificarán los activos de información del Organismo. Existen muchos tipos de activos, que incluyen:

a) información: bases de datos, archivos de datos, documentación, contratos, acuerdos;

b) activos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo, y utilitarios;

c) activos físicos: equipamiento de computación, equipamiento de comunicaciones, medios removibles y otros equipamientos;

d) instalaciones: edificios, ubicaciones físicas, tendido eléctrico, red de agua y gas, etc.;

e) servicios: servicios de cómputo y de comunicaciones, servicios generales, por ejemplo: calefacción, iluminación, energía, y aire acondicionado;

f) personas, y sus calificaciones, habilidades y experiencia;

g) activos intangibles, tales como la reputación y la imagen del Organismo

El inventario será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad de……….. (establecer período no mayor a 6 meses).

El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable de Unidad Organizativa.

8.1.2 Control: Propiedad de los activos

Toda la información y los activos junto a sus medios de procesamiento de información deben ser propiedad de un responsable designado en el organismo.

Se designarán los Propietarios de los activos identificados, quienes deben cumplir sus funciones de propietario, esto es:

a) informar sobre cualquier cambio que afecte el inventario de activos;

b) clasificar los activos en función a su valor;

c) definir los requisitos de seguridad de los activos;

d) velar por la implementación y el mantenimiento de los controles de seguridad requeridos en los activos.

Cabe aclarar que, si bien los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservarán la responsabilidad del cumplimiento de las mismas. La delegación de la administración por parte de los propietarios de los activos será documentada por los mismos y proporcionada al Responsable de Seguridad de la Información.

8.1.3 Control: Uso aceptable de los activos

Se identificarán, documentarán e implementarán reglas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de la información.

Todos los empleados, contratistas y usuarios de terceras partes deben seguir las reglas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de la misma, incluyendo:

a) correo electrónico,

b) sistemas de gestión,

c) estaciones de trabajo,

d) dispositivos móviles,

e) herramientas y equipamiento de publicación de contenidos,

f) etc.

8.2 Categoría: Clasificación de la información

Objetivo

Asegurar que la información reciba un nivel de protección apropiado.

La información debe ser clasificada para indicar la necesidad, prioridades y grado de protección esperado cuando se maneja la información.

La información tiene diversos grados de confidencialidad e importancia. Algunos ítems pueden requerir un nivel de protección adicional o manejo especial. Se debe utilizar un esquema de clasificación de información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de uso especiales.

8.2.1 Control: Directrices de clasificación

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

A continuación se establece la metodología de clasificación de la información propuesta en función a cada una de las mencionadas características:

Confidencialidad:

0. Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado del Organismo o no. PUBLICO

1. Información que puede ser conocida y utilizada por todos los empleados del Organismo y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el Organismo, el Sector Público Nacional o terceros. RESERVADA - USO INTERNO

2. Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas al Organismo, al Sector Público Nacional o a terceros. RESERVADA - CONFIDENCIAL

3. Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección del Organismo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros. RESERVADA SECRETA

Integridad:

0. Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria del Organismo.

1. Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para el Organismo, el Sector Público Nacional o terceros.

2. Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para el Organismo, el Sector Público Nacional o terceros.

3. Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al Organismo, al Sector Público Nacional o a terceros.

Disponibilidad:

0. Información cuya inaccesibilidad no afecta la operatoria del Organismo.

1. Información cuya inaccesibilidad permanente durante……….. (definir un plazo no menor a una semana) podría ocasionar pérdidas significativas para el Organismo, el Sector Público Nacional o terceros.

2. Información cuya inaccesibilidad permanente durante……….. (definir un plazo no menor a un día) podría ocasionar pérdidas significativas al Organismo, al Sector Público Nacional o a terceros.

3. Información cuya inaccesibilidad permanente durante……….. (definir un plazo no menor a una hora) podría ocasionar pérdidas significativas al Organismo, al Sector Público Nacional o a terceros.

Al referirse a pérdidas, se contemplan aquellas mesurables (materiales) y no mesurables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.).

Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:

CRITICIDAD BAJA: ninguno de los valores asignados superan el 1.

CRITICIDAD MEDIA: alguno de los valores asignados es 2.

CRITICIDAD ALTA: alguno de los valores asignados es 3.

Sólo el Propietario de la información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

• Asignarle una fecha de efectividad.

• Comunicárselo al depositario del recurso.

• Realizar los cambios necesarios para que los Usuarios conozcan la nueva clasificación.

Luego de clasificada la información, el propietario de la misma identificará los recursos asociados (sistemas, equipamiento, servicios, etc.) y los perfiles funcionales que deben tener acceso a la misma.

En adelante se mencionará como “información clasificada” (o “datos clasificados”) a aquella que se encuadre en los niveles 1, 2 o 3 de Confidencialidad.

8.2.2 Control: Etiquetado y manipulado de la información

Se definirán procedimientos para el rotulado y manejo de información, de acuerdo al esquema de clasificación definido. Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información:

- Copia;

- Almacenamiento;

- Transmisión por correo, fax, correo electrónico;

- Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, etc.).

- Transmisión a través de mecanismos de intercambio de archivos (FTP, almacenamiento masivo remoto, etc.).

Para cada uno de los niveles de clasificación, se deben definir los procedimientos de manejo seguros, incluyendo las actividades de procesamiento, almacenaje, transmisión, de-clasificación y destrucción.

8.3 Categoría: Gestión de medios

Objetivo

Evitar la divulgación no-autorizada; modificación, eliminación o destrucción de activos; y la interrupción de las actividades. Los medios se debieran controlar y proteger físicamente.

Se deben establecer los procedimientos de operación apropiados para proteger los documentos, medios de cómputo (por ejemplo, cintas y discos), entrada/salida de datos (input/output) y documentación del sistema de una divulgación no-autorizada, modificación, eliminación y destrucción.

8.3.1 Control: Administración de Medios Informáticos Removibles

El Responsable del Área Informática, con la asistencia del Responsable de Seguridad de la Información, implementará procedimientos para la administración de medios informáticos removibles, como cintas, discos, pen drives e informes impresos. El cumplimiento de los procedimientos se hará de acuerdo a la cláusula “9.1 Categoría: Requerimientos para el Control de Acceso”.

Se deben considerar las siguientes acciones para la implementación de los procedimientos:

a) Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por el Organismo.

b) Requerir autorización para retirar cualquier medio del Organismo y realizar un control de todos los retiros a fin de mantener un registro de auditoría.

c) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores y la criticidad de la información almacenada.

8.3.2 Control: Eliminación de Medios de Información

El Responsable del Área Informática, junto con el Responsable de Seguridad de la Información definirá procedimientos para la eliminación segura de los medios de soporte de información respetando la normativa vigente.

Los procedimientos deben considerar que los siguientes elementos requerirán almacenamiento y eliminación segura:

a) Documentos en papel.

b) Voces u otras grabaciones.

c) Papel carbónico.

d) Informes de salida.

e) Cintas de impresora de un solo uso.

f) Cintas magnéticas.

g) Discos u otros dispositivos removibles.

h) Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor).

i) Listados de programas.

j) Datos de prueba.

k) Documentación del sistema.

La evaluación del mecanismo de eliminación debe contemplar el tipo de dispositivo y la criticidad de la información contenida.

8.3.3 Control: Seguridad de los Medios en Tránsito

Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deben contemplar:

a) La utilización de medios de transporte o servicios de mensajería confiables. El Propietario de la Información a transportar determinará qué servicio de mensajería se utilizará conforme la criticidad de la información a transmitir.

b) Suficiente embalaje para envío de medios a través de servicios postales o de mensajería, siguiendo las especificaciones de los fabricantes o proveedores.

c) La adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas. Entre los ejemplos se incluyen:

1) Uso de recipientes cerrados.

2) Entrega en mano.

3) Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso).

4) En casos excepcionales, división de la mercadería a enviar en más de una entrega y envío por diferentes rutas.

9. Cláusula: Gestión de Accesos



Generalidades

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto-a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

Objetivo

Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información. Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

Controlar la seguridad en la conexión entre la red del Organismo y otras redes públicas o privadas. Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

Alcance

La Política definida en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos o servicios de información del Organismo, cualquiera sea la función que desempeñe.

Asimismo se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

Responsabilidad

El Responsable de Seguridad de la Información estará a cargo de:

Definir normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de computación móvil, trabajo remoto y reportes de incidentes relacionados; la respuesta a la activación de alarmas silenciosas; la revisión de registros de actividades (logs); y el ajuste de relojes de acuerdo a un estándar preestablecido.

- Definir pautas de utilización de Internet para todos los usuarios.

- Participar en la definición de normas y procedimientos de seguridad a implementar en el ambiente informático (ej.: sistemas operativos, servicios de red, enrutadores o gateways, etc.) y validarlos periódicamente.

- Controlar periódicamente la asignación de privilegios a usuarios.

- Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.

- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registración de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, alarmas silenciosas, desconexión de terminales por tiempo muerto, limitación del horario de conexión, registro de eventos, protección de puertos (físicos y lógicos), subdivisión de redes, control de conexiones a la red, control de ruteo de red, etc.

- Concientizar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo.

- Verificar periódicamente el cumplimiento de los procedimientos de revisión de registros de auditoría.

- Asistir a los usuarios que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma.

Los Propietarios de la Información estarán encargados de:

- Evaluar los riesgos a los cuales se expone la información con el objeto de:

• determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso.

• definir los eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión de los mismos.

- Aprobar y solicitar la asignación de privilegios a usuarios.

- Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.

- Definir un cronograma de depuración de registros de auditoría en línea.

Los Propietarios de la Información junto con la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, definirán un cronograma de depuración de logs y registros de auditoría en línea en función a normas vigentes y a sus propias necesidades.

Los Responsable de las Unidades Organizativas, junto con el Responsable de Seguridad de la Información, autorizarán el trabajo remoto del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con las normas vigentes. Asimismo autorizarán el acceso de los usuarios a su cargo a los servicios y recursos de red y a Internet.

El Responsable del Área Informática cumplirá las siguientes funciones:

- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.

- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.

- Evaluar el costo y el impacto de la implementación de “enrutadores”, “gateways” y/o firewalls adecuados para subdividir la red y recomendar el esquema apropiado.

- Implementar el control de puertos, de conexión a la red y de ruteo de red.

- Implementar el registro de eventos o actividades (logs) de usuarios de acuerdo a lo definido por los propietarios de la información, así como la depuración de los mismos.

- Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.

- Evaluar los riesgos sobre la utilización de las instalaciones de procesamiento de información, con el objeto de definir medios de monitoreo y tecnologías de identificación y autenticación de usuarios (Ej.: biometría, verificación de firma, uso de autenticadores de hardware).

- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operatoria.

- Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.

- Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal correspondiente.

- Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

El Comité de Seguridad de la Información aprobará el análisis de riesgos de la información efectuado. Asimismo, aprobará el período definido para el mantenimiento de los registros de auditoría generados.

Política

9.1 Categoría: Requerimientos para la Gestión de Acceso

Objetivo

Controlar el acceso a la información. Se debe controlar el acceso a la información, medios de procesamiento de la información y procesos sobre la base de los requerimientos del organismo y de seguridad. Las reglas de control del acceso deben tomar en cuenta las políticas para la divulgación y autorización de la información.

9.1.1 Control: Política de Gestión de Accesos

En la aplicación de gestión de acceso, se contemplarán los siguientes aspectos:

a) Identificar los requerimientos de seguridad de cada una de las aplicaciones.

b) Identificar toda la información relacionada con las aplicaciones.

c) Establecer criterios coherentes entre esta Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas y redes (Ver cláusula 8 Gestión de Activos).

d) Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.

e) Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.

f) Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones y dispositivos disponibles.

9.1.2 Control: Reglas de Gestión de Acceso

Las reglas de control de acceso especificadas, deben:

a) Indicar expresamente si las reglas son obligatorias u optativas

b) Establecer reglas sobre la premisa “Todo debe estar prohibido a menos que se permita expresamente” y no sobre la premisa inversa de “Todo está permitido a menos que se prohiba expresamente”.

c) Controlar los cambios en los rótulos de información que son iniciados automáticamente por herramientas de procesamiento de información, de aquellos que son iniciados a discreción del usuario (Ver cláusula 8 Gestión de Activos).

d) Controlar los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por el administrador.

e) Controlar las reglas que requieren la aprobación del administrador o del Propietario de la Información de que se trate, antes de entrar en vigencia, y aquellas que no requieren aprobación.

9.2 Categoría: Administración de Gestión de Usuarios

Objetivo

Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

Los procedimientos debieran abarcar todas las etapas en el ciclo de vida del acceso del usuario, desde el registro inicial de usuarios nuevos hasta la baja final de los usuarios que ya no requieren acceso a los sistemas y servicios de información.

9.2.1 Control: Registración de Usuarios

El Responsable de Seguridad de la Información definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender:

a) Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.

b) Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.

c) Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad del Organismo, por ejemplo que no compromete la segregación de funciones.

d) Entregar a los usuarios un detalle escrito de sus derechos de acceso.

e) Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.

f) Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.

g) Mantener un registro formal de todas las personas registradas para utilizar el servicio.

h) Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon del Organismo o sufrieron la pérdida/robo de sus credenciales de acceso.

i) Efectuar revisiones periódicas con el objeto de:

- cancelar identificadores y cuentas de usuario redundantes

- inhabilitar cuentas inactivas por más de……… (indicar período no mayor a 60 días)

- eliminar cuentas inactivas por más de………… (indicar período no mayor a 120 días)

En el caso de existir excepciones, deben ser debidamente justificadas y aprobadas.

j) Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.

k) Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados en caso de corresponder.

9.2.2 Control: Gestión de Privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

a) Identificar los privilegios asociados a cada producto del sistema, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.

b) Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.

c) Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.

d) Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados.

e) Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Responsable de Seguridad de la Información.

9.2.3 Control: Gestión de Contraseñas de Usuario

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

a) Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración bien puede estar incluida en el Compromiso de Confidencialidad.

b) Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez acreditada la identidad del usuario.

c) Generar contraseñas provisorias seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo formal cuando la reciban.

d) Almacenar las contraseñas sólo en sistemas informáticos protegidos.

e) Utilizar otras tecnologías de autenticación y autorización de usuarios, como ser la biométrica (por ejemplo verificación de huellas dactilares), verificación de firma, uso de autenticadores de hardware (como las tarjetas de circuito integrado), etc. El uso de esas herramientas se dispondrá cuando la evaluación de riesgos realizada por el Responsable de Seguridad de la Información conjuntamente con el Responsable del Área de Informática y el Propietario de la Información lo determine necesario (o lo justifique).

f) Configurar los sistemas de tal manera que:

- las contraseñas sean del tipo “password fuerte” y tengan……… (especificar cantidad no menor a 8 caracteres) caracteres,

- suspendan o bloqueen permanentemente al usuario luego de……… (especificar cantidad no mayor a 3) intentos de entrar con una contraseña incorrecta (debe pedir la rehabilitación ante quien corresponda),

- solicitar el cambio de la contraseña cada……… (especificar lapso no mayor a 45 días),

- impedir que las últimas……… (especificar cantidad no menor a 12) contraseñas sean reutilizadas,

- establecer un tiempo de vida mínimo de……… (especificar cantidad no mayor a 3) días para las contraseñas.

9.2.4 Control: Administración de Contraseñas Críticas

En los diferentes ambientes de procesamiento existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser instalación de plataformas o sistemas, habilitación

de servicios, actualización de software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual. El Responsable de Seguridad de la Información definirá procedimientos para la administración de dichas contraseñas críticas que contemplen lo siguiente:

a) Se definirán las causas que justificarán el uso de contraseñas críticas así como el nivel de autorización requerido.

b) Las contraseñas seleccionadas serán seguras, y su definición será efectuada como mínimo por dos personas, de manera que ninguna de ellas conozca la contraseña completa.

c) Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente.

d) La utilización de las contraseñas críticas será registrada, documentando las causas que determinaron su uso, así como el responsable de las actividades que se efectúen con la misma.

e) Cada contraseña crítica se renovará una vez utilizada y se definirá un período luego del cual la misma será renovada en caso de que no se la haya utilizado.

f) Se registrarán todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas. Dicho registro será revisado posteriormente por el Responsable de Seguridad de la Información.

9.2.5 Control: Revisión de Derechos de Acceso de Usuarios

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información de que se trate llevará a cabo un proceso formal, a intervalos regulares de……….. (Indicar periodicidad no mayor a 6 meses), a fin de revisar los derechos de acceso de los usuarios. Se deben contemplar los siguientes controles:

a) Revisar los derechos de acceso de los usuarios a intervalos de……….. (Especificar tiempo no mayor a 6 meses).

b) Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos de………….. (Especificar tiempo no mayor a 3 meses).

c) Revisar las asignaciones de privilegios a intervalos de………….. (Especificar tiempo no mayor a 6 meses), a fin de garantizar que no se obtengan privilegios no autorizados.

9.3 Categoría: Responsabilidades del Usuario

Objetivo

Evitar el acceso de usuarios no-autorizados, evitar poner en peligro la información y evitar el robo de información y los medios de procesamiento de la información.

La cooperación de los usuarios autorizados es esencial para una seguridad efectiva.

Los usuarios deben estar al tanto de sus responsabilidades para mantener controles de acceso efectivos, particularmente con relación al uso de claves secretas y la seguridad del equipo del usuario.

Se debe implementar una política de escritorio y pantalla limpios para reducir el riesgo de acceso no autorizado o daño a los papeles, medios y medios de procesamiento de la información.

9.3.1 Control: Uso de Contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

a) Mantener las contraseñas en secreto.

b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.

c) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el Responsable del Activo de Información de que se trate, que:

1. Sean fáciles de recordar.

2. No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.

3. No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.

e) Cambiar las contraseñas provisorias en el primer inicio de sesión (“log on”).

f) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.

g) Notificar de acuerdo a lo establecido en la cláusula 16 Gestión de Incidentes de Seguridad, cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas y en tránsito.

9.4 Categoría: Control de Acceso a Sistemas y Aplicaciones

Objetivo

Evitar el acceso no autorizado a los servicios de la red.

Se debe controlar el acceso a los servicios de redes internas y externas.

El acceso del usuario a las redes y servicios de las redes no deben comprometer la seguridad de los servicios de la red asegurando:

a) que existan las interfases apropiadas entre la red del Organismo y las redes de otras organizaciones, y redes públicas;

b) se apliquen los mecanismos de autenticación apropiados para los usuarios y el equipo;

c) el control del acceso del usuario a la información sea obligatorio.

9.4.1 Control: Política de Utilización de los Servicios de Red

Las conexiones no seguras a los servicios de red pueden afectar a todo el Organismo, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

El Responsable del Área Informática tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del titular de una Unidad Organizativa que lo solicite para personal de su incumbencia.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la administración y del control de seguridad del Organismo.

Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

a) Identificar las redes y servicios de red a los cuales se permite el acceso.

b) Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.

c) Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

Esta Política será coherente con la Política de Gestión de Accesos del Organismo.

9.4.2 Control: Camino Forzado

Las redes están diseñadas para permitir el máximo alcance de distribución de recursos y flexibilidad en la elección de la ruta a utilizar. Estas características también pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones del Organismo, o para el uso no autorizado de servicios de información. Por esto, el camino de las comunicaciones será controlado.

Se limitarán las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales el mismo se encuentra autorizado a acceder, mediante la implementación de controles en diferentes puntos de la misma.

A continuación se enumeran algunos ejemplos a considerar en caso de implementar estos controles a los sistemas existentes:

a) Asignar números telefónicos o líneas, en forma dedicada.

b) Establecer la conexión automática de puertos a gateways de seguridad o a sistemas de aplicación específicos.

c) Limitar las opciones de menú y submenú de cada uno de los usuarios.

d) Evitar la navegación ilimitada por la red.

e) Imponer el uso de sistemas de aplicación y/o gateways de seguridad específicos para usuarios externos de la red.

f) Controlar activamente las comunicaciones con origen y destino autorizados a través de un gateway, por ejemplo utilizando firewalls y generando alertas ante eventos no previstos.

g) Restringir el acceso a redes, estableciendo dominios lógicos separados, por ejemplo, redes privadas virtuales para grupos de usuarios dentro o fuera del Organismo.

Los requerimientos relativos a caminos forzados se basarán en la Política de Control de Accesos del Organismo El Responsable de Seguridad de la Información, conjuntamente con el Propietario de la Información de que se trate, realizará una evaluación de riesgos a fin de determinar los mecanismos de control que corresponda en cada caso.

9.4.3 Control: Autenticación de Usuarios para Conexiones Externas

Las conexiones externas son de gran potencial para accesos no autorizados a la información del Organismo. Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación. Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros. El Responsable de Seguridad de la Información, conjuntamente con el Propietario de la Información de que se trate, realizará una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

La autenticación de usuarios remotos puede llevarse a cabo utilizando:

a) Un método de autenticación físico (por ejemplo tokens de hardware), para lo que debe implementarse un procedimiento que incluya:

• Asignación de la herramienta de autenticación.

• Registro de los poseedores de autenticadores.

• Mecanismo de rescate al momento de la desvinculación del personal al que se le otorgó.

• Método de revocación de acceso del autenticador, en caso de compromiso de seguridad.

b) Un protocolo de autenticación (por ejemplo desafío/respuesta), para lo que debe implementarse un procedimiento que incluya:

• Establecimiento de las reglas con el usuario.

• Establecimiento de un ciclo de vida de las reglas para su renovación.

c) También pueden utilizarse líneas dedicadas privadas o una herramienta de verificación de la dirección del usuario de red, a fin de constatar el origen de la conexión.

Los procedimientos y controles de rellamada, o dial-back, pueden brindar protección contra conexiones no autorizadas a las instalaciones de procesamiento de información del Organismo. Al aplicar este tipo de control, el Organismo no debe utilizar servicios de red que incluyan desvío de llamadas. Si por alguna causa es preciso mantener el desvío de llamadas, no será posible aplicar el control de re-llamada. Asimismo, es importante que el proceso de re-llamada garantice que se produzca a su término, una desconexión real del lado del Organismo.

En caso de utilizarse sistemas de Voz sobre IP, deben ajustarse los controles a fin de que no sean utilizados para efectuar comunicaciones no autorizadas (ej.: bloqueo de puertos).

9.4.4 Control: Autenticación de Nodos

Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación del Organismo. Por consiguiente, las conexiones a sistemas informáticos remotos serán autenticadas. Esto es particularmente importante si la conexión utiliza una red que está fuera de control de la gestión de seguridad del Organismo. En el punto anterior se mencionan algunos ejemplos de autenticación y de cómo puede lograrse. La autenticación de nodos puede servir como un medio alternativo de autenticación de grupos de usuarios remotos, cuando éstos están conectados a un servicio informático seguro y compartido.

9.4.5 Control: Protección de los Puertos (Ports) de Diagnóstico Remoto

Muchas computadoras y sistemas de comunicación son instalados y administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado, con las mismas características del punto “9.4.3 Control: Autenticación de Usuarios para Conexiones Externas”. También para este caso debe tenerse en cuenta el punto “9.4.2 Control: Camino Forzado”.

9.4.6 Control: Subdivisión de Redes

Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados. Para esto se definirán y documentarán los perímetros de seguridad que sean convenientes. Estos perímetros se implementarán mediante la instalación de “gateways” con funcionalidades de “firewall” o redes privadas virtuales, para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado de acuerdo a la Política de Control de Accesos.

La subdivisión en dominios de la red tomará en cuenta criterios como los requerimientos de seguridad comunes de grupos de integrantes de la red, la mayor exposición de un grupo a peligros externos, separación física, u otros criterios de aglutinamiento o segregación preexistentes.

Basándose en la Política de Gestión de Accesos y los requerimientos de acceso (9.1 Categoría: Requerimientos para la Gestión de Acceso), el Responsable del Área Informática evaluará el costo relativo y el impacto en el desempeño que ocasione la implementación de enrutadores o gateways adecuados para subdividir la red. Luego decidirá, junto con el Responsable de Seguridad de la Información, el esquema más apropiado a implementar.

9.4.7 Control: Acceso a Internet

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto.

El Responsable de Seguridad de la Información definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por el Responsable de la Unidad Organizativa a cargo del personal que lo solicite. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios.

Se evaluará la conveniencia de generar un registro de los accesos de los usuarios a Internet, con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares. Dicho control será comunicado a los usuarios de acuerdo a lo establecido en el punto 6.1.5 Control: Acuerdos de confidencialidad. Para ello, el Responsable de Seguridad de la Información junto con el Responsable del Área de Informática analizarán las medidas a ser implementadas para efectivizar dicho control, como ser la instalación de “firewalls”, “proxies”, etc.

9.4.8 Control: Conexión a la Red

Sobre la base de lo definido en el punto “9.1 Categoría: Requerimientos para la gestión de accesos”, se implementarán controles para limitar la capacidad de conexión de los usuarios. Dichos controles se podrán implementar en los “gateways” que separen los diferentes dominios de la red.

Algunos ejemplos de los entornos a las que deben implementarse restricciones son:

a) Correo electrónico.

b) Transferencia de archivos.

c) Acceso interactivo.

d) Acceso a la red fuera del horario laboral.

9.4.9 Control: Ruteo de Red

En las redes compartidas, especialmente aquellas que se extienden fuera de los límites del Organismo, se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino. Adicionalmente, para este objetivo pueden utilizarse diversos métodos incluyendo entre otros autenticación de protocolos de ruteo, ruteo estático, traducción de direcciones y listas de control de acceso.

9.4.10 Control: Seguridad de los Servicios de Red

El Responsable de Seguridad de la Información junto con el Responsable del Área informática definirán las pautas para garantizar la seguridad de los servicios de red del Organismo, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.

- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.

- Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentarse.

- Instalar periódicamente las actualizaciones de seguridad.

Dicha configuración será revisada periódicamente por el Responsable de Seguridad de la Información.

9.5 Categoría: Control de Acceso al Sistema Operativo

Objetivo

Evitar el acceso no autorizado a los sistemas operativos.

Se deben utilizar medios de seguridad para restringir el acceso a los sistemas operativos a los usuarios no autorizados. Los medios deben tener la capacidad para:

a) autenticar a los usuarios autorizados, en concordancia con una política de control de acceso definida;

b) registrar los intentos exitosos y fallidos de autenticación del sistema;

c) registrar el uso de los privilegios especiales del sistema;

d) emitir alarmas cuando se violen las políticas de seguridad del sistema;

e) proporcionar los medios de autenticación apropiados;

f) cuando sea apropiado, restringir el tiempo de conexión de los usuarios

9.5.1 Control: Identificación Automática de Terminales

El Responsable de Seguridad de la Información junto con el Responsable del Área Informática realizará una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

Si del análisis realizado surgiera la necesidad de proveer un método de identificación de terminales, se redactará un procedimiento que indique:

a) El método de identificación automática de terminales utilizado.

b) El detalle de transacciones permitidas por terminal o dispositivo.

9.5.2 Control: Procedimientos de Conexión de Terminales.

El acceso a los servicios de información sólo será posible a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema informático será diseñado para minimizar la oportunidad de acceso no autorizado.

Este procedimiento, por lo tanto, debe divulgar la mínima información posible acerca del sistema, a fin de evitar proveer de asistencia innecesaria a un usuario no autorizado.

El procedimiento de identificación debe:

a) Mantener en secreto los identificadores de sistemas o aplicaciones hasta tanto se halla llevado a cabo exitosamente el proceso de conexión.

b) Desplegar un aviso general advirtiendo que sólo los usuarios autorizados pueden acceder a la computadora.

c) Evitar dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión.

d) Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta.

e) Limitar el número de intentos de conexión no exitosos permitidos y:

- Registrar los intentos no exitosos.

- Impedir otros intentos de identificación, una vez superado el límite permitido.

- Desconectar conexiones de comunicaciones de datos.

f) Limitar el tiempo máximo permitido para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión.

g) Desplegar la siguiente información, al completarse una conexión exitosa:

- Fecha y hora de la conexión exitosa anterior.

- Detalles de los intentos de conexión no exitosos desde la última conexión exitosa.

9.5.3 Control: Identificación y Autenticación de los Usuarios

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable, a fin de garantizar la trazabilidad de las transacciones. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

En circunstancias excepcionales, cuando existe un claro beneficio para el Organismo, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se documentará la justificación y aprobación del Propietario de la Información de que se trate.

Si se utilizará un método de autenticación físico (por ejemplo autenticadores de hardware), debe implementarse un procedimiento que incluya:

a) Asignar la herramienta de autenticación.

b) Registrar los poseedores de autenticadores.

c) Rescatar el autenticador al momento de la desvinculación del personal al que se le otorgó.

d) Revocar el acceso del autenticador, en caso de compromiso de seguridad.

9.5.4 Control: Sistema de Administración de Contraseñas

Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático. Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad.

El sistema de administración de contraseñas debe:

a) Imponer el uso de contraseñas individuales para determinar responsabilidades.

b) Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de las mismas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.

c) Imponer una selección de contraseñas de calidad según lo señalado en el punto “9.3.1 Control: Uso de Contraseñas”.

d) Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas.

e) Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.

f) Mantener un registro de las últimas 13 contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.

g) Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.

10. Cláusula: Criptografía



Generalidades

La criptografía se usa en forma primaria para proteger la información del riesgo de seguridad que la misma pueda ser interceptada por cualquier persona no autorizada.

Esto reduce la probabilidad de que partes no autorizadas puedan tener acceso a la información.

Se debe tener cuidado con los sistemas de encriptación que no protegen a toda la información para asegurar que aquella información clasificada como confidencial.

Objetivos

Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, no-repudio, la autenticidad y/o la integridad de la información.

Alcance

Esta Política se aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por el Organismo en donde residan los desarrollos mencionados.

Responsabilidad

El Responsable de Seguridad de la Información, junto con el Propietario de la Información, definirá en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, el Responsable de Seguridad de la información definirá junto con el Responsable del Área de Sistemas, los métodos de encripción a ser utilizados.

Asimismo, el Responsable de Seguridad de la Información cumplirá las siguientes funciones:

- Definir los procedimientos de administración de claves.

- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.

- Garantizar el cumplimiento de los requerimientos de seguridad para el software.

- Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso; y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

Política

10.1 Categoría: Cumplimiento de Requisitos Legales

Objetivo

Se utilizarán sistemas y técnicas criptográficas para la protección de la información en base a un análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad. Se debe desarrollar una política sobre el uso de controles criptográficos. Se debe establecer una gestión clave para sostener el uso de técnicas criptográficas.

10.1.1 Control: Política de Utilización de Controles Criptográficos

El Organismo establece la presente Política de uso de controles criptográficos, a fin de determinar su correcto uso. Para ello se indica que:

a) Se utilizarán controles criptográficos en los siguientes casos:

1) Para la protección de claves de acceso a sistemas, datos y servicios.

2) Para la transmisión de información clasificada, fuera del ámbito del Organismo.

3) Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el Responsable de Seguridad de la Información.

b) Se desarrollarán procedimientos respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.

c) El Responsable del Área Informática propondrá la siguiente asignación de funciones:

Función	Cargo
Implementación de la Política de Controles Criptográficos	
Administración de Claves	

d) Se utilizarán, como mínimo, los siguientes algoritmos de cifrado y tamaños de clave:

Cifrado Simétrico

Algoritmo	Longitud de Clave
AES	128/192/256
3DES	168 bits
IDEA	128 bits
RC4	128 bits
RC2	128 bits

Cifrado Asimétrico

Casos de Utilización	Algoritmo	Longitud de Clave
Para certificados utilizados en servicios relacionados a la firma digital (sellado de tiempo, almacenamiento seguro de documentos electrónicos, etc.)	RSA	2048 bits
	DSA	2048 bits
	ECDSA	210 bits
Para certificados de sitio seguro	RSA	1024 bits
Para certificados de Certificador o de información de estado de certificados	RSA	2048 bits
	DSA	2048 bits
	ECDSA	210 bits
Para certificados de usuario (personas físicas o jurídicas)	RSA	1024 bits
	DSA	1024 bits
	ECDSA	160 bits
Para digesto seguro	SHA-1	256 bits

Los algoritmos y longitudes de clave mencionados son los que a la fecha se consideran seguros. Se recomienda verificar esta condición periódicamente con el objeto de efectuar las actualizaciones correspondientes.

10.1.2 Control: Cifrado

Mediante la evaluación de riesgos que llevará a cabo el Propietario de la Información y el Responsable de Seguridad de la Información, se identificará el nivel requerido de protección, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.

Al implementar la Política del Organismo en materia criptográfica, se considerarán los controles aplicables a la exportación e importación de tecnología criptográfica.

10.1.3 Control: Firma Digital

Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos. Pueden aplicarse a cualquier tipo de documento que se procese electrónicamente. Se implementan mediante el uso de una técnica criptográfica sobre la base de dos claves relacionadas de manera única, donde una clave, denominada privada, se utiliza para crear una firma y la otra, denominada pública, para verificarla.

Se tomarán recaudos para proteger la confidencialidad de las claves privadas.

Asimismo, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública.

Los algoritmos de firma utilizados, como así también la longitud de clave a emplear, son los descriptos en la presente política.

Se recomienda que las claves criptográficas utilizadas para firmar digitalmente no sean empleadas en procedimientos de cifrado de información. Dichas claves deben ser resguardadas bajo el control exclusivo de su titular.

Al utilizar firmas y certificados digitales, se considerará la legislación vigente (Ley N° 25.506, el Decreto N° 2628/02 y el conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos) que describa las condiciones bajo las cuales una firma digital es legalmente válida.

En algunos casos podría ser necesario establecer acuerdos especiales para respaldar el uso de las firmas digitales. A tal fin se debe obtener asesoramiento legal con respecto al marco normativo aplicable y la modalidad del acuerdo a implementar. (Ver Cláusula 10.1.1 Control: Política de utilización de controles criptográficos, en el cuadro de cifrado asimétrico).

10.1.4 Control: Servicios de No Repudio

Estos servicios se utilizarán cuando sea necesario resolver disputas acerca de la ocurrencia de un evento o acción. Su objetivo es proporcionar herramientas para evitar que aquél que haya originado una transacción electrónica niegue haberla efectuado.

10.1.5 Control: Protección de claves criptográficas

Se implementará un sistema de administración de claves criptográficas para respaldar la utilización por parte del Organismo de los dos tipos de técnicas criptográficas, a saber:

a) Técnicas de clave secreta (criptografía simétrica), cuando dos o más actores comparten la misma clave y ésta se utiliza tanto para cifrar información como para descifrarla.

b) Técnicas de clave pública (criptografía asimétrica), cuando cada usuario tiene un par de claves: una clave pública (que puede ser revelada a cualquier persona) utilizada para cifrar y una clave privada (que debe mantenerse en secreto) utilizada para descifrar. Las claves asimétricas utilizadas para cifrado no deben ser las mismas que se utilizan para firmar digitalmente.

Todas las claves serán protegidas contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada.

Se aplicarán con éste propósito los algoritmos criptográficos enumerados en el punto 10.1.1 Control: Política de Utilización de Controles Criptográficos.

Se proporcionará una protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.

10.1.6 Control: Protección de Claves criptográficas: Normas y procedimientos

Se redactarán las normas y procedimientos necesarios para:

a) Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.

b) Generar y obtener certificados de clave pública de manera segura.

c) Distribuir claves de forma segura a los usuarios que corresponda, incluyendo información sobre cómo deben activarse cuando se reciban.

d) Almacenar claves, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados.

e) Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.

f) Revocar claves, incluyendo cómo deben retirarse o desactivarse las mismas, por ejemplo cuando las claves están comprometidas o cuando un usuario se desvincula del Organismo (en cuyo caso las claves también deben archivarse).

g) Recuperar claves pérdidas o alteradas como parte de la administración de la continuidad de las actividades del Organismo, por ejemplo para la recuperación de la información cifrada.

h) Archivar claves, por ejemplo, para la información archivada o resguardada.

i) Destruir claves.

j) Registrar y auditar las actividades relativas a la administración de claves.

A fin de reducir la probabilidad de compromiso, las claves tendrán fechas de inicio y caducidad de vigencia, definidas de manera que sólo puedan ser utilizadas por el lapso de……….. (indicar lapso no mayor a 12 meses).

Además de la administración segura de las claves secretas y privadas, debe tenerse en cuenta la protección de las claves públicas. Este problema es abordado mediante el uso de un certificado de clave pública. Este certificado se generará de forma que vincule de manera única la información relativa al propietario del par de claves pública/privada con la clave pública.

En consecuencia es importante que el proceso de administración de los certificados de clave pública sea absolutamente confiable. Este proceso deberá ser llevado a cabo por una entidad denominada Autoridad de Certificación (AC) o Certificador.

11. Cláusula: Física y Ambiental



Generalidades

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones del Organismo. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen tres conceptos a tener en cuenta: la protección física de accesos, la protección ambiental y el transporte, protección y mantenimiento de equipamiento y documentación.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible del Organismo, de accesos físicos no autorizados.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. Deben contemplarse tanto los riesgos en las instalaciones del Organismo como en instalaciones próximas a la sede del mismo que puedan interferir con las actividades.

El equipamiento donde se almacena información es susceptible de mantenimiento periódico, lo cual implica en ocasiones su traslado y permanencia fuera de las áreas protegidas del Organismo. Dichos procesos deben ser ejecutados bajo estrictas normas de seguridad y de preservación de la información almacenada en los mismos. Así también se tendrá en cuenta la aplicación de dichas normas en equipamiento perteneciente al Organismo pero situado físicamente fuera del mismo (“housing”) así como en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información al Organismo (“hosting”).

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados.

Gran cantidad de información manejada en las oficinas se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación; y para su destrucción cuando así lo amerite.

Objetivo

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información del Organismo.

Proteger el equipamiento de procesamiento de información crítica del Organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Organismo.

Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

Proporcionar protección proporcional a los riesgos identificados.

Alcance

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información del Organismo: instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, etc.

Responsabilidad

El Responsable de Seguridad de la Información definirá junto con el Responsable del Área Informática y los Propietarios de Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y controlará su implementación. Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en la presente Cláusula.

El Responsable del Área Informática asistirá al Responsable de Seguridad de la Información en la definición de las medidas de seguridad a implementar en áreas protegidas, y coordinará su implementación. Asimismo, controlará el mantenimiento del equipamiento informático de acuerdo a las indicaciones de proveedores tanto dentro como fuera de las instalaciones del Organismo.

Los Responsables de Unidades Organizativas definirán los niveles de acceso físico del personal del organismo a las áreas restringidas bajo su responsabilidad.

Los Propietarios de la Información autorizarán formalmente el trabajo fuera de las instalaciones con información de su incumbencia a los empleados del Organismo cuando lo crean conveniente.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información revisará los registros de acceso a las áreas protegidas.

Todo el personal del Organismo es responsable del cumplimiento de la política de pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario en las oficinas.

Política

11.1 Categoría: Áreas Seguras

Objetivo

Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales del Organismo.

Los medios de procesamiento de información crítica o confidencial deben ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Deben estar físicamente protegidos del acceso no autorizado, daño e interferencia.

11.1.1 Control: Perímetro de seguridad física

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las sedes del Organismo y de las instalaciones de procesamiento de información.

El Organismo utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera estarán definidas por el Responsable del Área Informática con el asesoramiento del Responsable de Seguridad de la Información, de acuerdo a la evaluación de riesgos efectuada.

Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda:

a) Definir y documentar claramente el perímetro de seguridad.

b) Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo mediante mecanismos de control, vallas, alarmas, cerraduras, etc.

c) Verificar la existencia de un área de recepción atendida por personal. Si esto no fuera posible se implementarán los siguientes medios alternativos de control de acceso físico al área o edificio:……… (indicar otros medios alternativos de control). El acceso a dichas áreas y edificios estará restringido exclusivamente al personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa.

d) Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo por incendio, humedad e inundación.

e) Identificar claramente todas las puertas de incendio de un perímetro de seguridad.

Un área segura puede ser una oficina con llave, o varias oficinas rodeadas por una barrera de seguridad física interna continua. Pueden ser necesarios barreras y perímetros adicionales para controlar el acceso físico entre las áreas con diferentes requerimientos de seguridad, dentro del mismo perímetro de seguridad

El Responsable de Seguridad de la Información llevará un registro actualizado de los sitios protegidos, indicando:

a) Identificación del Edificio y Área.

b) Principales elementos a proteger.

c) Medidas de protección física

11.1.2 Control: Controles físicos de entrada

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Responsable de Seguridad de la Información junto con el Responsable del Área Informática, a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

a) Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.

b) Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se utilizarán los siguientes controles de autenticación para autorizar y validar todos los accesos:………… (por ejemplo: personal de guardia con listado de personas habilitadas o por tarjeta magnética o inteligente y número de identificación personal (PIN), etc.). Se mantendrá un registro protegido para permitir auditar todos los accesos.

c) Implementar el uso de una identificación unívoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.

d) Revisar y actualizar cada……… (definir período no mayor a 6 meses) los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el Responsable de la Unidad Organizativa de la que dependa.

e) Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

11.1.3 Control: Seguridad de oficinas, despachos, instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones.

Se definen los siguientes sitios como áreas protegidas del Organismo

Areas Protegidas

………………………………

Se establecen las siguientes medidas de protección para áreas protegidas:

a) Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.

b) Establecer que los edificios o sitios donde se realicen actividades de procesamiento de información serán discretos y ofrecerán un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.

c) Ubicar las funciones y el equipamiento de soporte, por ejemplo: impresoras, fotocopiadoras, máquinas de fax, adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.

d) Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia. Se agregará protección externa a las ventanas, en particular las que se encuentran en planta baja o presenten riesgos especiales.

e) Implementar los siguientes mecanismos de control para la detección de intrusos:……………………… (detallar cuales). Los mismos serán instalados según estándares profesionales y probados periódicamente. Estos mecanismos de control comprenderán todas las puertas exteriores y ventanas accesibles.

f) Separar las instalaciones de procesamiento de información administradas por el Organismo de aquellas administradas por terceros.

g) Restringir el acceso público a las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible.

h) Almacenar los materiales peligrosos o combustibles en los siguientes lugares seguros a una distancia prudencial de las áreas protegidas del Organismo:…………… (incluir lista de lugares seguros). Los suministros, como los útiles de escritorio, no serán trasladados al área protegida hasta que sean requeridos.

i) Almacenar los equipos redundantes y la información de resguardo (back up) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal:…………………… (detallar ubicación).

11.1.4 Control: Protección contra amenazas externas y de origen ambiental

Se debe asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre.

Se debe prestar consideración a cualquier amenaza contra la seguridad presentada por locales vecinos; por ejemplo, un fuego en un edificio vecino, escape de agua en el techo o pisos en sótano o una explosión en la calle.

Se debe considerar los siguientes lineamientos para evitar el daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre:

a) los materiales peligrosos o combustibles deben ser almacenados a una distancia segura del área asegurada. Los suministros a granel como papelería no deben almacenarse en el área asegurada;

b) el equipo de reemplazo y los medios de respaldo debieran ubicarse a una distancia segura para evitar el daño de un desastre que afecte el local principal;

c) se debe proporcionar equipo contra-incendios ubicado adecuadamente.

11.1.5 Control: Trabajo en áreas seguras

Para incrementar la seguridad de las áreas protegidas, se establecen los siguientes controles y lineamientos adicionales. Esto incluye controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí:

a) Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.

b) Evitar la ejecución de trabajos por parte de terceros sin supervisión.

c) Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas.

d) Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que requiera acceder al área protegida, será otorgado solamente cuando sea necesario y se encuentre autorizado y monitoreado. Se mantendrá un registro de todos los accesos de personas ajenas.

e) Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.

f) Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que hayan sido formalmente autorizadas por el Responsable de dicho área o el Responsable del Área Informática y el Responsable de Seguridad de la Información.

g) Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

11.1.6 Control: Áreas de acceso público, de carga y descarga

Se controlarán las áreas de Recepción y Distribución, las cuales estarán aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados.

Para ello se establecerán controles físicos que considerarán los siguientes lineamientos:

a) Limitar el acceso a las áreas de depósito, desde el exterior de la sede del Organismo, sólo al personal previamente identificado y autorizado.

b) Diseñar el área de depósito de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.

c) Proteger todas las puertas exteriores del depósito cuando se abre la puerta interna.

d) Inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.

e) Registrar el material entrante al ingresar al sitio pertinente.

f) Cuando fuese posible, el material entrante debe estar segregado o separado en sus diferentes partes que lo constituyan.

11.2 Categoría: Seguridad de los equipos

Objetivo

Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades del Organismo.

Se debe proteger el equipo de amenazas físicas y ambientales.

11.2.1 Control: emplazamiento y protección de equipos

El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

a) Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.

b) Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.

c) Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.

d) Adoptar controles adecuados para minimizar el riesgo de amenazas potenciales, por:

Amenazas Potenciales	Controles
Robo o hurto	
Incendio	
Explosivos	
Humo	
Inundaciones o filtraciones de agua (o falta de suministro)	
Polvo	
Vibraciones	
Efectos químicos	
Interferencia en el suministro de energía eléctrica (cortes de suministro, variación de tensión)	
Radiación electromagnética	
Derrumbes	
Etc.	

Se deben establecer lineamientos sobre las actividades de comer, beber y fumar en la proximidad de los medios de procesamiento de la información.

Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información. Esta revisión se realizará cada:……………… (indicar periodicidad, no mayor a seis meses).

Se deben aplicar protección contra rayos a todos los edificios y se deben adaptar filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones.

Considerar asimismo el impacto de las amenazas citadas en el punto d) que tengan lugar en zonas próximas a la sede del Organismo.

11.2.2 Control: Instalaciones de suministro

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

a) Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.

b) Contar con un suministro de energía interrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas del Organismo. La determinación de dichas operaciones críticas, será el resultado del análisis de impacto realizado por el Responsable de Seguridad de la Información conjuntamente con los Propietarios de la Información con incumbencia. Los planes de contingencia contemplarán las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.

c) Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Debe realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir qué componentes será necesario abastecer de energía alternativa. Dicho análisis será realizado por el Responsable de Seguridad de la Información conjuntamente con los Propietarios de la Información. Se dispondrá de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado. Cuando el encendido de los generadores no sea automático, se asegurará que el tiempo de funcionamiento de la UPS permita el encendido manual de los mismos. Los generadores serán inspeccionados y probados periódicamente para asegurar que funcionen según lo previsto.

Asimismo, se procurará que los interruptores de emergencia se ubiquen cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica. Se proveerá de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Se implementará protección contra descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo a las normativas vigentes.

Las opciones para lograr la continuidad de los suministros de energía incluyen múltiples alimentaciones para evitar que una falla en el suministro de energía.

11.2.3 Control: Seguridad del cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño, mediante las siguientes acciones:

a) Cumplir con los requisitos técnicos vigentes de la República Argentina.

b) Utilizar pisoducto o cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información. En su defecto estarán sujetas a la siguiente protección alternativa:………… (indicar protección alternativa del cableado)

c) Proteger el cableado de red contra intercepción no autorizada o daño mediante los siguientes controles:……… (ejemplo: el uso de conductos o evitando trayectos que atraviesen áreas públicas).

d) Separar los cables de energía de los cables de comunicaciones para evitar interferencias.

e) Proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos blindados.

Para los sistemas sensibles o críticos………………… y………….. (detallar cuáles son), se implementarán los siguientes controles adicionales:

a) Instalar conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.

b) Utilizar rutas o medios de transmisión alternativos.

11.2.4 Control: Mantenimiento de los equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

a) Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Responsables del Área Informática. El Área de Informática mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.

b) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.

c) Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.

d) Registrar el retiro de equipamiento de la sede del Organismo para su mantenimiento.

e) Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

11.2.5 Control: Seguridad de los equipos fuera de las instalaciones

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito del Organismo, será autorizado por el responsable patrimonial. En el caso de que en el mismo se almacene información clasificada, debe ser aprobado además por el Propietario de la misma. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito del Organismo para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento. Asimismo, se mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito del Organismo, cuando sea conveniente.

Los riesgos de seguridad, por ejemplo: daño, robo o intercepción; puede variar considerablemente entre los edificios y se debe tomarlo en cuenta para evaluar los controles apropiados.

11.2.6 Control: Reutilización o retiro seguro de equipos

La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento. Los medios de almacenamiento conteniendo material sensible, por ejemplo discos rígidos no removibles, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda.

Los dispositivos que contengan información confidencial deben requerir una evaluación de riesgo para determinar si los ítems debieran ser físicamente destruidos en lugar de enviarlos a reparar o descartar.

11.2.7 Control: Retirada de materiales propiedad del organismo

El equipamiento, la información y el software no serán retirados de la sede del Organismo sin autorización formal.

Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos del Organismo, las que serán llevadas a cabo por............. (indicar el Área responsable). El personal será puesto en conocimiento de la posibilidad de realización de dichas comprobaciones.

Los empleados deben saber que se llevan a cabo chequeos inesperados, y los chequeos se deben realizar con la debida autorización de los requerimientos legales y reguladores.

11.2.8 Control: Políticas de Pantallas Limpias

Los usuarios deben garantizar que los equipos desatendidos sean protegidos adecuadamente.

Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

El Responsable de Seguridad de la Información debe coordinar con el Área de Recursos Humanos las tareas de concientización a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

Los usuarios cumplirán con las siguientes pautas:

a) Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.

b) Proteger las PC's o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

11.2.9 Control: Políticas de Escritorios Limpios

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Se aplicarán los siguientes lineamientos:

a) Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.

b) Guardar bajo llave la información sensible o crítica del Organismo (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.

c) Desconectar de la red / sistema / servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o copia de las llaves de seguridad utilizadas en el sector a su cargo. Tales elementos se encontrarán protegidos en sobre cerrado o caja de seguridad para impedir accesos no autorizados, debiendo dejarse constancia de todo acceso a las mismas, y de los motivos que llevaron a tal acción.

d) Proteger los puntos de recepción y envío de correo postal y las máquinas de fax no atendidas.

e) Bloquear las fotocopiadoras (o protegerlas de alguna manera del uso no autorizado) fuera del horario normal de trabajo.

f) Retirar inmediatamente la información sensible o confidencial, una vez impresa.

12. Cláusula: Seguridad en las Operaciones



Generalidades

La proliferación de software malicioso, como virus, troyanos, etc., hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas.

Es conveniente separar los ambientes de desarrollo, prueba y operaciones de los sistemas del Organismo, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen en el ámbito operativo, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.

Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones:

Alcance

Todas las instalaciones de procesamiento de información del Organismo.

Responsabilidad

El Responsable de Seguridad de la información tendrá a su cargo, entre otros:

• Definir procedimientos para el control de cambios a los procesos operativos documentados, los sistemas e instalaciones de procesamiento de información, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.

• Establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva. Verificar que dichos procedimientos de aprobación de software incluyan aspectos de seguridad para todas las aplicaciones.

• Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.

• Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados en las redes del Organismo.

• Desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

• Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

El Responsable del Área Informática tendrá a su cargo lo siguiente:

• Controlar la existencia de documentación actualizada relacionada con los procedimientos de operaciones.

• Evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades.

• Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.

• Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario.

• Controlar la realización de las copias de resguardo de información, así como la prueba periódica de su restauración.

• Asegurar el registro de las actividades realizadas por el personal operativo, para su posterior revisión.

• Implementar los controles de seguridad definidos (software malicioso y accesos no autorizados).

• Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento, como cintas, discos, casetes e informes impresos y para la eliminación segura de los mismos.

• Participar en el tratamiento de los incidentes de seguridad, de acuerdo a los procedimientos establecidos.

El Responsable de Seguridad de la información junto con el Responsable del Área Informática y el Responsable del Área Jurídica del Organismo evaluarán los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

Cada Propietario de la Información, junto con el Responsable de Seguridad de la Información y el Responsable del Área Informática, determinará los requerimientos para resguardar la información por la cual es responsable. Asimismo, aprobará los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, revisará las actividades que no hayan sido posibles segregar. Asimismo, revisará los registros de actividades del personal operativo.

Política

12.1 Categoría: Procedimientos y Responsabilidades operativas

Objetivo

Asegurar la operación correcta y segura de los medios de procesamiento de la información.

Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información. Esto incluye el desarrollo de los procedimientos de operación apropiados

12.1.1 Control: Documentación de los Procedimientos

Operativos

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Responsable de Seguridad de la Información.

Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

a) Procesamiento y manejo de la información.

b) Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.

c) Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.

d) Restricciones en el uso de utilitarios del sistema.

e) Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.

f) Instrucciones especiales para el manejo de "salidas", como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.

g) Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

Se preparará adicionalmente documentación sobre procedimientos referidos a las siguientes actividades:

a) Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.

b) Instalación y mantenimiento de las plataformas de procesamiento.

c) Monitoreo del procesamiento y las comunicaciones.

d) Inicio y finalización de la ejecución de los sistemas.

e) Programación y ejecución de procesos.

f) Gestión de servicios.

g) Resguardo de información.

h) Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.

i) Remplazo o cambio de componentes del ambiente de procesamiento y comunicaciones.

j) Uso del correo electrónico.

12.1.2 Control: Cambios en las Operaciones

Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio debe ser evaluado previamente en aspectos técnicos y de seguridad.

El Responsable de Seguridad de la Información controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. El Responsable del Área Informática evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

Se retendrá un registro de auditoría que contenga toda la información relevante de cada cambio implementado.

Los procedimientos de control de cambios contemplarán los siguientes puntos:

a) Identificación y registro de cambios significativos.

b) Evaluación del posible impacto de dichos cambios.

c) Aprobación formal de los cambios propuestos.

d) Planificación del proceso de cambio.

e) Prueba del nuevo escenario.

f) Comunicación de detalles de cambios a todas las personas pertinentes.

g) Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

12.1.3 Control: Planificación de la Capacidad

El Responsable del Área Informática, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados. Para ello tomará en cuenta además los nuevos requerimientos de los sistemas así como las tendencias actuales y proyectadas en el procesamiento de la información del Organismo para el período estipulado de vida útil de cada componente. Asimismo, informará las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva.

12.1.4 Control: Separación de entornos de desarrollo, pruebas y operacionales

Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado productivo.

Para ello, se tendrán en cuenta los siguientes controles:

a) Ejecutar el software de desarrollo y de producción, en diferentes ambientes de operaciones, equipos, o directorios.

b) Separar las actividades de desarrollo y prueba, en entornos diferentes.

c) Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente de producción, cuando no sean indispensables para el funcionamiento del mismo.

d) Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.

e) Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes.

f) El personal de desarrollo no tendrá acceso al ambiente productivo. De ser extrema dicha necesidad, se establecerá un procedimiento de emergencia para la autorización, documentación y registro de dichos accesos.

12.2 Categoría: Protección contra el malware (código malicioso)

Objetivo

Proteger la integridad del software y la integración. Se requiere tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados. El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos; como ser, entre otros, virus Troyanos, bombas lógicas, etc. Los usuarios deben estar al tanto de los peligros de los códigos maliciosos. Cuando sea apropiado, los gerentes deben introducir controles para evitar, detectar y eliminar los códigos maliciosos y controlar los códigos móviles.

12.2.1 Control: Control contra el malware (código malicioso)

El Responsable de Seguridad de la Información definirá controles de detección y prevención para la protección contra software malicioso. El Responsable del Área Informática, o el personal designado por éste, implementara dichos controles.

El Responsable de Seguridad de la Información desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios. Estos controles deben considerar establecer políticas y procedimientos formales que contemplen las siguientes acciones:

a) Prohibir la instalación y uso de software no autorizado por el Organismo (Ver 18.1.2 Control: Derecho de Propiedad Intelectual).

b) Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio (ej: dispositivos portátiles), señalando las medidas de protección a tomar.

c) Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, como medida precautoria y rutinaria.

d) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).

e) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos del Organismo, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.

f) Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.

g) Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.

h) Concientizar al personal acerca del problema de los falsos antivirus (rogues) y las cadenas falsas (hoax) y de cómo proceder frente a los mismos.

i) Redactar normas de protección y habilitación de puertos de conexión de dispositivos móviles y sus derechos de acceso.

12.2.2 Control: Código Móvil

En caso que el código móvil sea autorizado, se debe garantizar que la configuración asegure que el código móvil autorizado opere de acuerdo a una configuración de seguridad claramente definida, previniendo que el código móvil no autorizado sea ejecutado.

Asimismo, se implementarán acciones para la protección contra acciones maliciosas resultantes de la ejecución no autorizada de código móvil, como ser:

a) ejecución del código móvil en un ambiente lógicamente aislado;

b) bloqueo del uso de código móvil;

c) bloqueo de la recepción de código móvil;

d) activación de medidas técnicas como sea disponible en un sistema específico para asegurar que el código móvil es gestionado;

e) control de los recursos disponibles para el acceso del código móvil;

f) implementación de controles criptográficos para autenticar de forma unívoca el código móvil.

12.3 Categoría: Resguardo (backup)

Objetivo

Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.

Se deben establecer los procedimientos de rutina para implementar la política de respaldo acordada y la estrategia (ver también Cláusula 17.1 Categoría: Gestión de Continuidad del Organismo) para tomar copias de respaldo de los datos y practicar su restauración oportuna.

12.3.1 Control: Resguardo de la Información

El Responsable del Área Informática, de Seguridad de la Información y los Propietarios de Información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información.

El Responsable del Área Informática dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración e integridad. Para esto se debe contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico del Organismo. Los sistemas de resguardo deben probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades del organismo, según el punto (ver también Cláusula 17.1 Categoría: Gestión de Continuidad del Organismo).

Se definirán procedimientos para el resguardo de la información, que deben considerar los siguientes puntos:

a) Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.

b) Establecer un esquema de remplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor, y asegurando la destrucción de los medios desechados.

c) Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deben retener al menos tres generaciones o ciclos de información de resguardo para la información y el software esenciales para el Organismo. Para la definición de información mínima a ser resguardada en el sitio remoto, se debe tener en cuenta el nivel de clasificación otorgado a la misma, en términos de disponibilidad y requisitos legales a los que se encuentre sujeta.

d) Asignar a la información de resguardo un nivel de protección física y ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.

e) Probar periódicamente los medios de resguardo.

f) Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

12.4 Categoría: Registro y Monitoreo

Objetivo

Detectar las actividades de procesamiento de información no autorizadas.

Se deben monitorear los sistemas y se deben reportar los eventos de seguridad de la información. Se deben utilizar bitácoras de operador y se deben registrar las fallas para asegurar que se identifiquen los problemas en los sistemas de información. Una organización debe cumplir con todos los requerimientos legales relevantes aplicables a sus actividades de monitoreo y registro.

Se debe utilizar el monitoreo del sistema para chequear la efectividad de los controles adoptados y para verificar la conformidad con un modelo de política de acceso.

12.4.1 Control: Registro de eventos

Se producirán y mantendrán registros de auditoría en los cuales se registren las actividades, excepciones, y eventos de seguridad de la información de los usuarios, por un período acordado para permitir la detección e investigación de incidentes.

Se debe evaluar la registración, en los mencionados registros, de la siguiente información:

a) identificación de los usuarios;

b) fechas, tiempos, y detalles de los eventos principales, por ejemplo, inicio y cierre de sesión;

c) identidad del equipo o la ubicación si es posible;

d) registros de intentos de acceso al sistema exitosos y fallidos;

e) registros de intentos de acceso a los datos u otro recurso, exitosos y rechazados;

f) cambios a la configuración del sistema;

g) uso de privilegios;

h) uso de utilitarios y aplicaciones de sistemas;

i) archivos accedidos y el tipo de acceso;

j) direcciones de redes y protocolos;

k) alarmas que son ejecutadas por el sistema de control de accesos;

l) activación y desactivación de los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusos.

12.4.2 Control: Protección del registro de información

Se implementarán controles para la protección de los registros de auditoría contra cambios no autorizados y problemas operacionales, incluyendo:

a) alteraciones de los tipos de mensajes que son grabados;

b) edición o eliminación de archivos de registro;

Exceso de la capacidad de almacenamiento de los archivos de registro, resultando en la falla para registrar los eventos o sobrescribiendo eventos registrados en el pasado.

12.4.3 Control: Registro del Administrador y del Operador

Se registrarán y revisarán periódicamente en particular las actividades de los administradores y operadores de sistema incluyendo:

a) cuenta de administración u operación involucrada;

b) momento en el cual ocurre un evento (éxito o falla);

c) información acerca del evento (por ejemplo, los archivos manipulados) o las fallas (por ejemplo, los errores ocurridos y las acciones correctivas tomadas);

d) procesos involucrados.

12.4.4 Control: Sincronización de Relojes

A fin de garantizar la exactitud de los registros de auditoría, al menos los equipos que realicen estos registros, deben tener una correcta configuración de sus relojes.

Para ello, se dispondrá de un procedimiento de ajuste de relojes, el cual indicará también la verificación de los relojes contra una fuente externa del dato y la modalidad de corrección ante cualquier variación significativa.

12.5 Categoría: Control de Software Operacional

Objetivo

Garantizar la seguridad de los archivos del sistema.

Se debe controlar el acceso a los archivos del sistema y el código fuente del programa, y los proyectos TI. Asimismo, las actividades de soporte se debieran realizar de una manera segura.

12.5.1 Control: Instalación de software en sistemas operacionales

Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.

• Toda aplicación, desarrollada por el Organismo o por un tercero tendrá un único Responsable designado formalmente por el Responsable del Área Informática.

• Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.

• El Responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de la función de “implementador” al personal de su área que considere adecuado, quien tendrá como funciones principales:

a) Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.

b) Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.

c) Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del sector encargado del testeo y del usuario final.

d) Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

Otros controles a realizar son:

a) Guardar sólo los ejecutables en el ambiente de producción.

b) Llevar un registro de auditoría de las actualizaciones realizadas.

c) Retener las versiones previas del sistema, como medida de contingencia.

d) Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y conformidades pertinentes, las pruebas previas a realizarse, etc.

e) Denegar, cuando correspondiere, permisos de modificación al implementador sobre los programas fuentes bajo su custodia.

Evitar, que la función de implementador sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.

12.6 Categoría: Administración de vulnerabilidades técnicas

Objetivo

Se implementará la gestión de las vulnerabilidades técnicas de forma efectiva, sistemática y repetible, con mediciones que confirmen su efectividad. Dichas consideraciones incluirán los sistemas operativos, y cualquier otra aplicación en uso.

12.6.1 Control: Administración de vulnerabilidades técnicas

Se obtendrá información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, la exposición del Organismo a tales vulnerabilidades evaluadas, y se tomarán las medidas necesarias para tratar los riesgos asociados.

Para ello se contará con un inventario de software donde se detalle información de versiones del mismo así como datos del proveedor y responsable interno.

El proceso de gestión de las vulnerabilidades técnicas debe comprender:

a) Definición de roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas;

b) Procedimientos de identificación de vulnerabilidades técnicas potenciales;

c) Definición de una línea de tiempo para reaccionar ante las notificaciones de las vulnerabilidades técnicas potencialmente relevantes;

d) Definición de prioridades para la atención de necesidades relacionadas con actualizaciones de seguridad;

e) Identificación de los riesgos asociados y las acciones a llevar a cabo ante vulnerabilidades identificadas;

f) Identificación de los riesgos asociados a la instalación de parches;

g) Aprobación y evaluación de los parches antes de que sean instalados para garantizar que son efectivos y que no resultan en efectos secundarios que no puedan ser tolerados;

h) Consideración de controles alternativos en caso de inexistencia de parches;

i) Generación y mantenimiento de un registro de auditoría para todos los procedimientos emprendidos;

j) Seguimiento y evaluación regular del proceso de gestión de las vulnerabilidades técnicas para garantizar su efectividad y eficiencia;

12.6.2 Control: Restricciones en la instalación de software

Se deben establecer e implementar:

• las reglas que rigen la instalación de software por parte de los usuarios y poner en vigencia una política estricta sobre qué tipo de software pueden instalar los usuarios.

La instalación no controlada de software en dispositivos computacionales puede dar pie a la introducción de vulnerabilidades y a la fuga de información, a la falta de integridad u otros incidentes de seguridad de información o bien a la transgresión de derechos de propiedad intelectual.

12.7 Categoría: Consideraciones sobre la auditoría de los sistemas de información

Objetivo

Asegurar el cumplimiento de minimizar el impacto de las actividades de auditoría en los sistemas operacionales.

12.7.1 Control: Controles de auditoría de los sistemas de información

Cuando se realicen actividades de auditoría que involucren verificaciones de los sistemas en producción, se tomarán recaudos en la planificación de los requerimientos y tareas, y se acordará con las áreas involucradas a efectos de minimizar el riesgo de interrupciones en las operaciones.

Se contemplarán los siguientes puntos:

a) Acordar con el Área que corresponda los requerimientos de auditoría.

b) Controlar el alcance de las verificaciones. Esta función será realizada por el responsable de auditoría.

c) Limitar las verificaciones a un acceso de sólo lectura del software y datos de producción. Caso contrario, se tomarán los resguardos necesarios a efectos de aislar y contrarrestar los efectos de las modificaciones realizadas, una vez finalizada la auditoría. Por ejemplo:

• Eliminar archivos transitorios.

• Eliminar entidades ficticias y datos incorporados en archivos maestros.

• Revertir transacciones.

• Revocar privilegios otorgados.

d) Identificar claramente los recursos de tecnologías de información (TI) para llevar a cabo las verificaciones, los cuales serán puestos a disposición de los auditores. A tal efecto, la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información completará el siguiente formulario, el cual debe ser puesto en conocimiento de las áreas involucradas:

Recursos de TI a utilizar en la Verificación	
Sistemas de información	....
Base de datos	....
Hardware	....
Software de Auditoría	....
Medios Magnéticos	....
Personal de Auditoría	....
Interlocutores de las Áreas de Informática	....
Interlocutores de las Áreas Usuarias	....
Conexiones a Red	....
....	....

e) Identificar y acordar los requerimientos de procesamiento especial o adicional.

f) Monitorear y registrar todos los accesos, a fin de generar una pista de referencia. Los datos a resguardar deben incluir como mínimo:

• Fecha y hora.

• Puesto de trabajo.

• Usuario.

• Tipo de acceso.

• Identificación de los datos accedidos.

• Estado previo y posterior.

• Programa y/o función utilizada.

g) Documentar todos los procedimientos de auditoría, requerimientos y responsabilidades.

13. Cláusula: Gestión de Comunicaciones



Generalidades

Los sistemas de información están comunicados entre sí, tanto dentro del Organismo como con terceros fuera de él. Por lo tanto es necesario establecer criterios de seguridad en las comunicaciones que se establezcan.

Las comunicaciones establecidas permiten el intercambio de información, que debe estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

Alcance

Todas las instalaciones de procesamiento y transmisión de información del Organismo.

Responsabilidad

El Responsable de Seguridad de la información tendrá a su cargo, entre otros:

• Definir y documentar una norma clara con respecto al uso del correo electrónico.

• Controlar los mecanismos de distribución y difusión de información dentro del Organismo.

• Desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

• Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

El Responsable del Área Informática tendrá a su cargo lo siguiente:

• Controlar la existencia de documentación actualizada relacionada con los procedimientos de comunicaciones.

• Asegurar el registro de las actividades realizadas por el personal operativo, para su posterior revisión.

• Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento, como cintas, discos, casetes e informes impresos y para la eliminación segura de los mismos.

El Responsable de Seguridad de la información junto con el Responsable del Área Informática y el Responsable del Área Jurídica del Organismo evaluarán los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

Cada Propietario de la Información, junto con el Responsable de Seguridad de la Información y el Responsable del Área Informática, determinará los requerimientos para resguardar la información por la cual es responsable. Asimismo, aprobará los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, revisará las actividades que no hayan sido posibles segregar. Asimismo, revisará los registros de actividades del personal operativo.

Política

13.1 Categoría: Gestión de la Red

Objetivo

Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicancias legales, monitoreo y protección.

También se pueden requerir controles adicionales para proteger la información confidencial que pasa a través de redes públicas.

13.1.1 Control: Redes

El Responsable de Seguridad de la Información definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes del Organismo, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

a) Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias, la que será llevada a cabo por el responsable establecido en el punto “6.1.3 Control: Asignación de responsabilidad de la seguridad de la información”.

b) Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.

c) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

El Responsable del Área Informática implementará dichos controles.

13.1.2 Control: Seguridad de Servicio de red

El Responsable de Seguridad de la Información junto con el Responsable del Área Informática definirán las pautas para garantizar la seguridad de los servicios de red del Organismo, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:

• Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.

• Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.

• Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.

• Instalar periódicamente las actualizaciones de seguridad.

• Dicha configuración será revisada periódicamente por el Responsable de Seguridad de la Información.

13.2 Categoría: Transferencia de información

Objetivo

Mantener la seguridad en el intercambio de información dentro del Organismo y con cualquier otra entidad externa.

Los intercambios de información dentro de las organizaciones se deben basar en una política formal de intercambio, seguida en línea con los acuerdos de intercambio, y debiera cumplir con cualquier legislación relevante (ver 18 Cláusula: Cumplimiento).

Se deben establecer los procedimientos y estándares para proteger la información y los medios físicos que contiene la información en tránsito.

13.2.1 Control: Procedimientos y controles de intercambio de la información

Se establecerán procedimientos y controles formales para proteger el intercambio de información a través del uso de todos los tipos de instalaciones de comunicación, considerando lo siguiente:

a) Protección de la información intercambiada de la intercepción, copiado, modificación, de que sea mal dirigida, y de su destrucción.

b) detección de y la protección contra el código malicioso que puede ser transmitido a través del uso de comunicaciones electrónicas.

c) definición del uso aceptable de las instalaciones de comunicación electrónicas.

d) uso seguro de comunicaciones inalámbricas.

e) responsabilidades del empleado, contratista y cualquier otro usuario de no comprometer a la organización, por ejemplo, a través de la difamación, hostigamiento, personificación, reenvío de cadenas de comunicación epistolar, compras no autorizadas y cualquier otro medio (ej.: redes sociales).

f) uso de técnicas criptográficas para proteger la confidencialidad, integridad y la autenticidad de la información.

g) directrices de retención y eliminación para toda la correspondencia en concordancia con las leyes y regulaciones relevantes, locales y nacionales.

h) instrucción del personal sobre las precauciones que deben tomar a la hora de transmitir información del Organismo.

13.2.2 Control: Acuerdos de Intercambio de Información

Cuando se realicen acuerdos entre organizaciones para el intercambio de información y software, se especificarán el grado de sensibilidad de la información del Organismo involucrada y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos:

a) Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.

b) Procedimientos de notificación de emisión, transmisión, envío y recepción.

c) Normas técnicas para el empaquetado y la transmisión.

d) Pautas para la identificación del prestador del servicio de correo.

e) Responsabilidades y obligaciones en caso de pérdida, exposición o divulgación no autorizada de datos.

f) Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida.

g) Términos y condiciones de la licencia bajo la cual se suministra el software.

h) Información sobre la propiedad de la información suministrada y las condiciones de su uso.

i) Normas técnicas para la grabación y lectura de la información y del software.

j) Controles especiales que puedan requerirse para proteger ítems sensibles, (claves criptográficas, etc.).

13.2.3 Control: Seguridad de la Mensajería

La mensajería electrónica como el correo electrónico, el intercambio de datos electrónicos (EDI por sus siglas en inglés), la mensajería instantánea y las redes sociales juegan un muy importante en las comunicaciones organizacionales. La mensajería electrónica tiene diferentes riesgos que las comunicaciones basadas en papel.

Se considerarán las siguientes medidas de seguridad en los mensajes electrónicos:

•protección de mensajes por el acceso no autorizado, modificaciones o denegación de servicio;

• correcta asignación de la dirección y el transporte del mensaje;

• confiabilidad y disponibilidad general del servicio;

• consideraciones legales, por ejemplo, requerimientos para firmas electrónicas;

• obtención de aprobación previa al uso de los servicios públicos externos tales como mensajería instantánea o el compartir archivos;

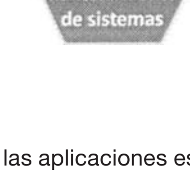
• niveles altos de controles de autenticación para los accesos desde las redes públicamente accesibles.

13.2.4 Control: Acuerdos de confidencialidad.

Se definirán, implementarán y revisarán regularmente los acuerdos de confidencialidad o de no divulgación para la protección de la información del Organismo. Dichos acuerdos deben responder a los requerimientos de confidencialidad o no divulgación del Organismo, los cuales serán revisalos periódicamente. Asimismo, deben cumplir con toda legislación o normativa que alcance al Organismo en materia de confidencialidad de la información.

Dichos acuerdos deben celebrarse tanto con el personal del organismo como con aquellos terceros que se relacionen de alguna manera con su información.

14. Cláusula: Adquisición, desarrollo y mantenimiento de sistemas



Generalidades

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad.

Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deben diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

Dado que los analistas y programadores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer / alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente al responsable.

Asimismo, es necesaria una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

Objetivo

Asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información.

Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

Definir los métodos de protección de la información crítica o sensible.

Alcance

Esta Política se aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por el Organismo en donde residan los desarrollos mencionados.

Responsabilidad

El Responsable de Seguridad de la Información junto con el Propietario de la Información y la Unidad de Auditoría Interna, definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.

El Responsable de Seguridad de la Información, junto con el Propietario de la Información, definirá en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, el Responsable de Seguridad de la Información definirá junto con el Responsable del Área de Sistemas, los métodos de encripción a ser utilizados.

Asimismo, el Responsable de Seguridad de la Información cumplirá las siguientes funciones:

• Definir los procedimientos de administración de claves.

• Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.

• Garantizar el cumplimiento de los requerimientos de seguridad para el software.

• Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso; y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

El Responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de funciones de "implementador" y "administrador de programas fuentes" al personal de su área que considere adecuado, cuyas responsabilidades se detallan en la presente cláusula. Asimismo, verificará el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas.

El Área de Sistemas propondrá quiénes realizarán la administración de las técnicas criptográficas y claves.

El Responsable del Área de Administración incorporará aspectos relacionados con el licenciamiento, la calidad del software y la seguridad de la información en los contratos con terceros por el desarrollo de software. El Responsable del Área Jurídica participará en dicha tarea.

Política

14.1 Categoría: Requerimientos de Seguridad de los Sistemas

Objetivo

Garantizar que la seguridad sea una parte integral de los sistemas de información.

Los sistemas de información incluyen sistemas de operación, infraestructura, aplicaciones operativas, productos de venta masiva, servicios y aplicaciones desarrolladas por el usuario. El diseño e implementación del sistema de información que soporta el proceso operativo puede ser crucial para la seguridad. Se deben identificar y acordar los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información.

14.1.1 Control: Análisis y Especificaciones de los Requerimientos de seguridad

Esta Política se implementa para incorporar seguridad a los sistemas de información (propios o de terceros) y a las mejoras o actualizaciones que se les incorporen.

Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles manuales de apoyo.

Se deben tener en cuenta las siguientes consideraciones:

a) Definir un procedimiento para que durante las etapas de análisis y diseño del sistema, se incorporen a los requerimientos, los correspondientes controles de seguridad. Este procedimiento debe incluir una etapa de evaluación de riesgos previa al diseño, para definir los requerimientos de seguridad e identificar los controles apropiados. En esta tarea deben participar las áreas usuarias, de sistemas, de seguridad informática y auditoría, especificando y aprobando los controles automáticos a incorporar al sistema y las necesidades de controles manuales complementarios. Las áreas involucradas podrán solicitar certificaciones y evaluaciones independientes para los productos a utilizar.

b) Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas.

c) Considerar que los controles introducidos en la etapa de diseño, son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.

14.1.2 Control: Seguridad de servicios aplicativos en redes públicas

Se controlarán los mecanismos de distribución y difusión tales como documentos, computadoras, dispositivos de computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general (analógica o digital), multimedia, servicios o instalaciones postales, equipos de fax, etc.

Al interconectar dichos medios, se considerarán las implicancias en lo que respecta a la seguridad y a las actividades propias del Organismo, incluyendo:

a) Vulnerabilidades de la información en los sistemas de oficina, por ejemplo la grabación de llamadas telefónicas o teleconferencias, la confidencialidad de las llamadas, el almacenamiento de faxes, la apertura o distribución del correo.

b) Procedimientos y controles apropiados para administrar la distribución de información, por ejemplo el uso de boletines electrónicos institucionales.

c) Exclusión de categorías de información sensible del Organismo, si el sistema no brinda un adecuado nivel de protección.

d) Limitación del acceso a la información de las actividades que desarrollan determinadas personas, por ejemplo aquellas que trabaja en proyectos sensibles.

e) La aptitud del sistema para dar soporte a las aplicaciones del Organismo, como la comunicación de órdenes o autorizaciones.

f) Categorías de personal y contratistas o terceros a los que se permite el uso del sistema y las ubicaciones desde las cuales se puede acceder al mismo.

g) Restricción de acceso a determinadas instalaciones a específicas categorías de usuarios.

h) Identificación de la posición o categoría de los usuarios, por ejemplo empleados del Organismo o contratistas, en directorios accesibles por otros usuarios.

i) Retención y resguardo de la información almacenada en el sistema.

j) Requerimientos y disposiciones relativos a sistemas de soporte de reposición de información previa.

14.1.3 Control: Protección de servicios de aplicativos

Se tomarán recaudos para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada que podría dañar la reputación del Organismo que emite la publicación. Es posible que la información de un sistema de acceso público, por ejemplo la información en un servidor Web accesible por Internet, deba cumplir con ciertas normas de la jurisdicción en la cual se localiza el sistema o en la cual tiene lugar la transacción electrónica. Se implementará un proceso de autorización formal antes de que la información se ponga a disposición del público, estableciéndose en todos los casos los encargados de dicha aprobación.

Todos los sistemas de acceso público deben prever que:

a) La información se obtenga, procese y proporcione de acuerdo a la normativa vigente, en especial la Ley de Protección de Datos Personales.

b) La información que se ingresa al sistema de publicación, o aquella que procesa el mismo, sea procesada en forma completa, exacta y oportuna.

c) La información sensible o confidencial sea protegida durante el proceso de recolección y su almacenamiento.

d) El acceso al sistema de publicación no permita el acceso accidental a las redes a las cuales se conecta el mismo.

e) El responsable de la publicación de información en sistemas de acceso público sea claramente identificado.

f) La información se publique teniendo en cuenta las normas establecidas al respecto.

g) Se garantice la validez y vigencia de la información publicada.

14.2 Categoría: Seguridad en los Sistemas de Aplicación

Objetivo

Para evitar la pérdida, modificación o uso inadecuado de los datos pertenecientes a los sistemas de información, se establecerán controles y registros de auditoría, verificando:

a) La validación efectiva de datos de entrada.

b) El procesamiento interno.

c) La autenticación de mensajes (interfaces entre sistemas)

d) La validación de datos de salida.

14.2.1 Control: Validación de Datos de Entrada

Se definirá un procedimiento que durante la etapa de diseño, especifique controles que aseguren la validez de los datos ingresados, tan cerca del punto de origen como sea posible, controlando también datos permanentes y tablas de parámetros.

Este procedimiento considerará los siguientes controles:

a) Control de secuencia.

b) Control de monto límite por operación y tipo de usuario.

c) Control del rango de valores posibles y de su validez, de acuerdo a criterios predeterminados.

d) Control de paridad.

e) Control contra valores cargados en las tablas de datos.

f) Controles por oposición, de forma tal que quien ingrese un dato no pueda autorizarlo y viceversa.

Por otra parte, se llevarán a cabo las siguientes acciones:

a) Se definirá un procedimiento para realizar revisiones periódicas de contenidos de campos claves o archivos de datos, definiendo quién lo realizará, en qué forma, con qué método, quiénes deben ser informados del resultado, etc.

b) Se definirá un procedimiento que explicite las alternativas a seguir para responder a errores de validación en un aplicativo.

c) Se definirá un procedimiento que permita determinar las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

14.2.2 Control: Controles de Procesamiento Interno

Se definirá un procedimiento para que durante la etapa de diseño, se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.

Para ello se implementarán:

a) Procedimientos que permitan identificar el uso y localización en los aplicativos, de funciones de incorporación y eliminación que realizan cambios en los datos.

b) Procedimientos que establezcan los controles y verificaciones necesarios para prevenir la ejecución de programas fuera de secuencia o cuando falle el procesamiento previo.

c) Procedimientos que establezcan la revisión periódica de los registros de auditoría o alertas de forma de detectar cualquier anomalía en la ejecución de las transacciones.

d) Procedimientos que realicen la validación de los datos generados por el sistema.

e) Procedimientos que verifiquen la integridad de los datos y del software cargado o descargado entre computadoras.

f) Procedimientos que controlen la integridad de registros y archivos.

g) Procedimientos que verifiquen la ejecución de los aplicativos en el momento adecuado.

h) Procedimientos que aseguren el orden correcto de ejecución de los aplicativos, la finalización programada en caso de falla, y la detención de las actividades de procesamiento hasta que el problema sea resuelto.

14.2.3 Control: Autenticación de Mensajes

Cuando una aplicación tenga previsto el envío de mensajes que contengan información clasificada, se implementarán los controles criptográficos determinados en el punto 10.1.1 Control: Política de Utilización de Controles Criptográficos.

14.2.4 Control: Validación de Datos de Salidas

Se establecerán procedimientos para validar la salida de los datos de las aplicaciones, incluyendo:

a) Comprobaciones de la razonabilidad para probar si los datos de salida son plausibles.

b) Control de conciliación de cuentas para asegurar el procesamiento de todos los datos.

c) Provisión de información suficiente, para que el lector o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información.

d) Procedimientos para responder a las pruebas de validación de salidas.

e) Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

14.3 Categoría: Seguridad de los Archivos del Sistema

Objetivo

Se garantizará que los desarrollos y actividades de soporte a los sistemas se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo.

14.3.1 Control: Software Operativo

Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.

• Toda aplicación, desarrollada por el Organismo o por un tercero tendrá un único Responsable designado formalmente por el Responsable del Área Informática.

• Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.

• El Responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de la función de “implementador” al personal de su área que considere adecuado, quien tendrá como funciones principales:

a) Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.

b) Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.

c) Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del sector encargado del testeo y del usuario final.

d) Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

Otros controles a realizar son:

e) Guardar sólo los ejecutables en el ambiente de producción.

f) Llevar un registro de auditoría de las actualizaciones realizadas.

g) Retener las versiones previas del sistema, como medida de contingencia.

h) Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y conformes pertinentes, las pruebas previas a realizarse, etc.

i) Denegar permisos de modificación al implementador sobre los programas fuentes bajo su custodia.

j) Evitar, que la función de implementador sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.

14.3.2 Control: Protección de los Datos de Prueba del Sistema

Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo. Para proteger los datos de prueba se establecerán normas y procedimientos que contemplen lo siguiente:

Prohibir el uso de bases de datos operativas. En caso contrario se deben despersonalizar los datos antes de su uso. Aplicar idénticos procedimientos de control de acceso que en la base de producción. Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización.

Eliminar inmediatamente, una vez completadas las pruebas, la información operativa utilizada.

14.3.3 Control: Cambios a Datos Operativos

La modificación, actualización o eliminación de los datos operativos serán realizados a través de los sistemas que procesan dichos datos y de acuerdo al esquema de control de accesos implementado en los mismos. Una modificación por fuera de los sistemas a un dato, almacenado ya sea en un archivo o base de datos, podría poner en riesgo la integridad de la información.

Los casos en los que no fuera posible la aplicación de la precedente política, se considerarán como excepciones. El Responsable de Seguridad de la Información definirá procedimientos para la gestión de dichas excepciones que contemplarán lo siguiente:

a) Se generará una solicitud formal para la realización de la modificación, actualización o eliminación del dato.

b) El Propietario de la Información afectada y el Responsable de Seguridad de la Información aprobarán la ejecución del cambio evaluando las razones por las cuales se solicita.

c) Se generarán cuentas de usuario de emergencia para ser utilizadas en la ejecución de excepciones. Las mismas serán protegidas mediante contraseñas, sujetas al procedimiento de administración de contraseñas críticas y habilitadas sólo ante un requerimiento de emergencia y por el lapso que ésta dure.

d) Se designará un encargado de implementar los cambios, el cual no será personal del área de Desarrollo. En el caso de que esta función no pueda ser segregada, se aplicarán controles adicionales de acuerdo a lo establecido en la Cláusula 7 Recursos Humanos.

e) Se registrarán todas las actividades realizadas con las cuentas de emergencia. Dicho registro será revisado posteriormente por el Responsable de Seguridad de la Información.

14.3.4 Control: Acceso a las Bibliotecas de Programas fuentes

Para reducir la probabilidad de alteración de programas fuentes, se aplicarán los siguientes controles:

a) El Responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda la función de “administrador de programas fuentes” al personal de su área que considere adecuado, quien tendrá en custodia los programas fuentes y debe:

• Proveer al Área de Desarrollo los programas fuentes solicitados para su modificación, manteniendo en todo momento la correlación programa fuente / ejecutable.

• Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, Analista Responsable que autorizó, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).

• Verificar que el Analista Responsable que autoriza la solicitud de un programa fuente sea el designado para la aplicación, rechazando el pedido en caso contrario. Registrar cada solicitud aprobada.

• Administrar las distintas versiones de una aplicación.

• Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador.

b) Denegar al “administrador de programas fuentes” permisos de modificación sobre los programas fuentes bajo su custodia.

c) Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.

d) Establecer que el implementador de producción efectuará la generación del programa objeto o ejecutable que estará en producción (compilación), a fin de garantizar tal correspondencia.

e) Desarrollar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática.

f) Evitar que la función de “administrador de programas fuentes” sea ejercida por personal que pertenezca al sector de desarrollo y/o mantenimiento.

g) Prohibir la guarda de programas fuentes históricos (que no sean los correspondientes a los programas operativos) en el ambiente de producción.

h) Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.

i) Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos por el Organismo en los procedimientos que surgen de la presente política.

14.4 Categoría: Seguridad de los Procesos de Desarrollo y Soporte

Objetivo

Esta Política provee seguridad al software y a la información del sistema de aplicación, por lo tanto se controlarán los entornos y el soporte dado a los mismos.

14.4.1 Control: Procedimiento de Control de Cambios

A fin de minimizar los riesgos de alteración de los sistemas de información, se implementarán controles estrictos durante la implementación de cambios imponiendo el cumplimiento de procedimientos formales. Éstos garantizarán que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

Para ello se establecerá un procedimiento que incluya las siguientes consideraciones:

a) Verificar que los cambios sean propuestos por usuarios autorizados y respete los términos y condiciones que surjan de la licencia de uso.

b) Mantener un registro de los niveles de autorización acordados.

c) Solicitar la autorización del Propietario de la Información, en caso de tratarse de cambios a sistemas de procesamiento de la misma.

d) Efectuar un análisis de riesgos del cambio.

e) Determinar los requisitos de seguridad para el cambio.

f) Analizar el impacto de los cambios sobre los controles de seguridad existentes.

g) Obtener aprobación formal por parte del Responsable del Área Informática para las tareas detalladas, antes que comiencen las tareas.

h) Solicitar la revisión del Responsable de Seguridad de la Información para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.

i) Efectuar las actividades relativas al cambio en el ambiente de desarrollo.

j) Obtener la aprobación por parte del usuario autorizado y del área de pruebas mediante pruebas en el ambiente correspondiente.

k) Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.

l) Mantener un control de versiones para todas las actualizaciones de software.

m) Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.

n) Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria.

o) Garantizar que sea el implementador quien efectúe el pasaje de los objetos modificados al ambiente operativo, de acuerdo a lo establecido en “14.3.1 Control: Software Operativo”.

En el Anexo a la presente cláusula se presenta un esquema modelo de segregación de ambientes de procesamiento.

14.4.2 Control: Revisión Técnica de los Cambios en el sistema Operativo

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

Para ello, se definirá un procedimiento que incluya:

a) Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.

b) Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación.

c) Asegurar la actualización del Plan de Continuidad de las Actividades del Organismo.

14.4.3 Control: Restricción del Cambio de Paquetes de Software

En caso de considerarlo necesario la modificación de paquetes de software suministrados por proveedores, y previa autorización del Responsable del Área Informática, se debe:

a) Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.

b) Determinar la conveniencia de que la modificación sea efectuada por el Organismo, por el proveedor o por un tercero.

c) Evaluar el impacto que se produciría si el Organismo se hace cargo del mantenimiento.

d) Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

14.4.4 Control: Canales Ocultos y Código Malicioso

Un canal oculto puede exponer información utilizando algunos medios indirectos y desconocidos. El código malicioso está diseñado para afectar a un sistema en forma no autorizada y no requerida por el usuario.

En este sentido, se redactarán normas y procedimientos que incluyan:

a) Adquirir programas a proveedores acreditados o productos ya evaluados.

b) Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.

c) Controlar el acceso y las modificaciones al código instalado.

d) Utilizar herramientas para la protección contra la infección del software con código malicioso.

e) Ejecutar controles y tests de evaluación de seguridad periódicamente y, en especial, previo a su puesta en producción.

14.4.5 Control: Desarrollo Externo de Software

Para el caso que se considere la tercerización del desarrollo de software, se establecerán normas y procedimientos que contemplen los siguientes puntos:

a) Acuerdos de licencias, propiedad de código y derechos conferidos (Ver 18.1.2 Derechos de Propiedad Intelectual).

b) Requerimientos contractuales con respecto a la calidad y seguridad del código y la existencia de garantías.

c) Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.

d) Verificación del cumplimiento de las condiciones de seguridad.

e) Acuerdos de custodia de los fuentes del software (y cualquier otra información requerida) en caso de quiebra y/o inhabilidad de la tercera parte.

14.5 Categoría: Gestión de vulnerabilidades técnicas

Objetivo

Se implementará la gestión de las vulnerabilidades técnicas de forma efectiva, sistemática y repetible, con mediciones que confirmen su efectividad. Dichas consideraciones incluirán los sistemas operativos, y cualquier otra aplicación en uso.

14.5.1 Control: Vulnerabilidades técnicas

Se obtendrá información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, la exposición del Organismo a tales vulnerabilidades evaluadas, y se tomarán las medidas necesarias para tratar los riesgos asociados.

Para ello se contará con un inventario de software donde se detalle información de versiones del mismo así como datos del proveedor y responsable interno.

El proceso de gestión de las vulnerabilidades técnicas debe comprender:

a) Definición de roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas;

b) Procedimientos de identificación de vulnerabilidades técnicas potenciales;

c) Definición de una línea de tiempo para reaccionar ante las notificaciones de las vulnerabilidades técnicas potencialmente relevantes;

d) Definición de prioridades para la atención de necesidades relacionadas con actualizaciones de seguridad;

e) Identificación de los riesgos asociados y las acciones a llevar a cabo ante vulnerabilidades identificadas;

f) Identificación de los riesgos asociados a la instalación de parches;

g) Aprobación y evaluación de los parches antes de que sean instalados para garantizar que son efectivos y que no resultan en efectos secundarios que no puedan ser tolerados;

h) Consideración de controles alternativos en caso de inexistencia de parches;

i) Generación y mantenimiento de un registro de auditoría para todos los procedimientos emprendidos;

j) Seguimiento y evaluación regular del proceso de gestión de las vulnerabilidades técnicas para garantizar su efectividad y eficiencia;

Información Complementaria

Para cumplir con esta Política, en lo referente a los puntos “Seguridad de los Archivos del Sistema y “Seguridad de los Procesos de Desarrollo y Soporte”, se sugiere implementar un modelo de separación de funciones entre los distintos ambientes involucrados.

Toda aplicación generada en el sector de desarrollo o adquirida a un proveedor es, en algún momento, implementada en un ambiente de producción. Los controles de esta transferencia deben ser rigurosos a fin de asegurar que no se instalen programas fraudulentos. Es conveniente implementar algún software para la administración de versiones y para la transmisión de programas entre los ambientes definidos, con un registro asociado para su control.

A continuación se presenta un modelo ideal formado por tres ambientes que debe ser adaptado a las características propias de cada Organismo, teniendo en cuenta las capacidades instaladas, los recursos y el equipamiento existente.

Ambiente de Desarrollo

Es donde se desarrollan los programas fuentes y donde se almacena toda la información relacionada con el análisis y diseño de los sistemas. El analista o programador (desarrollador) tiene total dominio sobre el ambiente. Puede recibir algún fuente para modificar, quedando registrado en el sistema de control de versiones que administra el “administrador de programas fuentes”.

El desarrollador realiza las pruebas con los datos de la base de desarrollo. Cuando considera que el programa está terminado, lo pasa al ambiente de pruebas junto con la documentación requerida que le entregará al implementador de ese ambiente.

Ambiente de Pruebas

El implementador de este ambiente recibe el programa y la documentación respectiva y realiza una prueba general con un lote de datos para tal efecto, junto con el usuario de ser posible.

El testeador realiza las pruebas con los datos de la base de pruebas. Si no detectan errores de ejecución, los resultados de las rutinas de seguridad son correctos de acuerdo a las especificaciones y considera que la documentación presentada es completa, entonces remite el programa fuente al implementador de producción por medio del sistema de control de versiones y le entrega las instrucciones. Caso contrario, vuelve atrás el ciclo devolviendo el programa al desarrollador, junto con un detalle de las observaciones.

Ambiente de Producción

Es donde se ejecutan los sistemas y se encuentran los datos productivos. Los programas fuentes certificados se guardan en un repositorio de fuentes de producción, almacenándolos mediante un sistema de control de versiones que maneja el “administrador de programas fuentes” y donde se dejan los datos del programador que hizo la modificación, fecha, hora y tamaño de los programas fuentes y objetos o ejecutables.

El “implementador” compila el programa fuente dentro del ambiente de producción en el momento de realizar el pasaje para asegurar de esta forma que hay una correspondencia biunívoca con el ejecutable en producción y luego se elimina, dejándolo en el repositorio productivo de programas fuentes.

Deben aplicarse procedimientos de la misma naturaleza y alcance para las modificaciones de cualquier otro elemento que forme parte del sistema, por ejemplo: modelo de datos de la base de datos o cambios en los parámetros, etc. Las modificaciones realizadas al software de base (Sistemas Operativos, Motores de bases de datos, Productos middleware) deben cumplir idénticos pasos, sólo que las implementaciones las realizarán los propios administradores.

Cabe aclarar que tanto el personal de desarrollo, como el proveedor de los aplicativos, no deben tener acceso al ambiente de producción, así como tampoco a los datos reales para la realización de las pruebas en el Ambiente de Prueba. Para casos excepcionales, se debe documentar adecuadamente la autorización, los trabajos realizados y monitorearlos en todo momento.

15. Cláusula: Relaciones con Proveedores



Generalidades

Los proveedores del Organismo deben ser gestionados en lo que respecta a los aspectos de seguridad que tienen que ver con el establecimiento y el acuerdo de todos los requisitos de seguridad de la información del organismo.

Objetivo

Establecer y mantener el nivel acordado de seguridad de información y prestación de servicios conforme a los acuerdos del proveedor.

Alcance

Los dos grandes puntos del alcance son:

• asegurar la protección de la información del organismo que es accedida por los proveedores, cumpliendo con el nivel de seguridad establecido.

• el mantenimiento del nivel acordado de seguridad de información y prestación de servicios conforme a los acuerdos del proveedor.

Responsabilidad

El Responsable de Seguridad de la Información, junto con el Propietario de la Información, deben definir en función a la criticidad de la información, los requerimientos de protección en lo referente al acceso de la información de los proveedores durante todo su ciclo de vida con el organismo. Asimismo todo responsable de las áreas legales, compras o que gestionen los contratos con proveedores, deben garantizar que en los mismos se definan y se acuerden los niveles de seguridad establecidos por el organismo.

Política

15.1 Categoría: Seguridad de la información en las relaciones con el proveedor

Objetivo

Garantizar y asegurar la protección de la información del organismo que es accedida por los proveedores, cumpliendo con el nivel de seguridad establecido.

15.1.1 Control: Política de seguridad de la información para las relaciones con el proveedor

Se deben acordar los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso de los proveedores a los activos del organismo con el proveedor y se deben documentar debidamente.

El organismo debe identificar e imponer controles de seguridad de la información para abordar específicamente el acceso de los proveedores a la información del organismo en una política.

Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de equipamiento de Trabajo del Organismo, contemplarán los siguientes aspectos:

a) la identificación y la documentación de los tipos de proveedores, es decir, los servicios de TI, las utilidades de logística, los servicios financieros, los componentes de la infraestructura de TI y a quiénes autorizará al organismo para acceder a su información;

b) un proceso y ciclo de vida estandarizado para administrar las relaciones con los proveedores;

c) la definición de los tipos de acceso a la información que se les permitirá a los distintos tipos de proveedores y el monitoreo y control del acceso;

d) requisitos mínimos de seguridad de la información para cada tipo de información y tipo de acceso para servir de base para los acuerdos individuales con los proveedores en base a las necesidades del organismo y los requisitos y su perfil de riesgo;

e) procesos y procedimientos para monitorear la adherencia a los requisitos de seguridad de información establecidos para cada tipo de proveedor y tipo de acceso, incluida la revisión de terceros y la validación de productos;

f) controles de precisión y nivel de detalles para garantizar la integridad de la información o el procesamiento de información que entrega cualquiera de las partes;

g) tipos de obligaciones aplicables a los proveedores para proteger la información;

h) manejo de incidentes y contingencias asociadas con el acceso a los proveedores, incluidas las responsabilidades del organismo y los proveedores;

i) resiliencia y, en caso de ser necesario, disposiciones de recuperación y contingencia para garantizar la disponibilidad de la información o el procesamiento de información proporcionado por cualquiera de las partes;

j) capacitación de concientización para el personal del organismo involucrado en las adquisiciones sobre políticas, procesos y procedimientos correspondientes;

k) capacitación de concientización para el personal del organismo que interactúa con el personal de los proveedores en cuanto a las reglas adecuadas sobre el compromiso y el comportamiento en base al tipo de proveedor y el nivel de acceso del proveedor a los sistemas y la información del organismo;

l) que las condiciones sobre los controles y requisitos de seguridad de la información se documentarán en un acuerdo firmado por ambas partes;

m) administración de las transiciones necesarias de información, instalaciones de procesamiento de información y cualquier otra cosa que se deba mover y, garantizando que se mantiene la seguridad de la información a través de todo el período de transición.

15.1.2 Control: Abordar la seguridad dentro de los acuerdos del proveedor

Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información del organismo.

Se deben establecer y documentar acuerdos con los proveedores para garantizar que no existen malos entendidos entre el organismo y el proveedor en cuanto a las obligaciones de ambas partes para cumplir con los requisitos de seguridad de la información pertinentes.

A continuación se definen los términos para incluir en los acuerdos a fin de y poder satisfacer los requisitos de seguridad de la información identificados:

a) descripción de la información que se debe proporcionar o a la que se debe acceder y los métodos para proporcionar o acceder a la información;

b) clasificación de la información de acuerdo al esquema de clasificación del organismo; y si es necesario también realizar el mapeo entre el esquema propio del organismo y el esquema de clasificación del proveedor;

c) requisitos legales y normativos, incluida la protección de datos personales, los derechos de propiedad intelectual y una descripción de sobre cómo se garantizará si se cumplen;

d) obligación de cada parte contractual de implementar un conjunto de controles acordados incluido el control de acceso, la revisión de desempeño, el monitoreo, los informes y la auditoría;

e) reglas de uso aceptable de la información, incluido en uso inaceptable en caso de ser necesario;

f) una lista explícita del personal autorizado para acceder a o recibir la información o los procedimientos o condiciones del organismo para su autorización y el retiro de la autorización, para el acceso a o la recepción de la información del organismo al personal del proveedor;

g) políticas de seguridad de la información pertinentes al contrato específico;

h) requisitos y procedimientos de la administración de incidentes (en especial la notificación y la colaboración durante la remediación de incidentes);

i) requisitos de capacitación y concientización para procedimientos específicos y requisitos de seguridad de la información, es decir, para la respuesta ante incidentes y procedimientos de autorización;

j) normativas pertinentes para la subcontratación, incluidos los controles que se deben implementar;

k) socios de acuerdos pertinentes, incluida una persona de contacto para los asuntos de seguridad de la información;

l) requisitos de selección, si existe alguno, para el personal del proveedor para realizar los procedimientos de selección y notificación si no se ha completado la selección o si los resultados dan pie a dudas o inquietudes;

m) derecho a auditar los procesos y los controles del proveedor relacionados al acuerdo;

n) procesos de resolución de defectos y resolución de conflictos;

o) obligación del proveedor a entregar periódicamente un informe independiente sobre la efectividad de los controles y un acuerdo sobre la corrección oportuna de los asuntos pertinentes indicados en el informe;

p) obligaciones del proveedor para cumplir con los requisitos de seguridad del organismo.

15.1.3 Control: Cadena de suministro de tecnologías de la información y comunicaciones

Se deben incluir en los acuerdos con los proveedores, los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.

Se deben incluir los siguientes temas en los acuerdos con el proveedor sobre la seguridad de la cadena de suministro:

a) definir los requisitos de seguridad de la información que se aplicarán a la adquisición de tecnologías, productos o servicios de información y comunicación además de los requisitos de seguridad de la información para las relaciones con el proveedor;

b) para los servicios de tecnología de información y comunicación, que requieren que los usuarios propaguen los requisitos de seguridad del organismo en toda la cadena de suministro si los proveedores realizan subcontrataciones para partes del servicio de tecnología de información y comunicación proporcionados al organismo;

c) para los productos de tecnología de información y comunicación que requieren que los proveedores propaguen las prácticas de seguridad correspondientes a través de toda la cadena de suministro si estos productos incluyen componentes comprados a otros proveedores;

d) implementación de un proceso de monitoreo y métodos aceptables para validar que los productos y servicios de tecnología de información y comunicación se adhieren a los requisitos de seguridad establecidos;

e) implementación de un proceso para identificar los componentes de los productos o servicios que son fundamentales para mantener la funcionalidad y que, por lo tanto, requiere una mayor atención y escrutinio cuando se desarrollan fuera del organismo, especialmente si el proveedor del nivel superior externalice los aspectos de los componentes de productos o servicios a otros proveedores;

f) obtención de una garantía de que los componentes críticos y su origen se pueden rastrear en toda la cadena de suministros;

g) obtener la garantía de que los productos de tecnología de información y comunicación entregados funcionan según lo esperado sin ninguna función inesperada o no deseada;

h) definición de las reglas para compartir la información en cuanto a la cadena de suministro y cualquier posible problema y compromiso entre el organismo y los proveedores;

i) implementación de procesos específicos para administrar el ciclo de vida de los componentes de tecnología de información y comunicación junto con la disponibilidad y los riesgos de seguridad asociados. Esto incluye los riesgos de los componentes que ya no están disponibles debido a que los proveedores ya no están en el negocio o a que ya no proporcionan estos componentes debido a los avances de la tecnología.

15.2 Categoría: Administración de prestación de servicios de proveedores

Objetivo

Garantizar el mantenimiento del nivel acordado de seguridad de información y prestación de servicios conforme a los acuerdos del proveedor.

15.2.1 Control: Supervisión y Revisión de los servicios del proveedor

Se llevará a cabo el seguimiento, control y revisión de los servicios de las terceras partes asegurando que se encuentran adheridos a los términos de seguridad de la información y las condiciones definidas en los acuerdos, y que los incidentes de seguridad de la información y los problemas son manejados en forma apropiada.

El Organismo mantendrá control suficiente y visión general de todos los aspectos de seguridad para la información sensible o crítica, o de las instalaciones de procesamiento de información accedidas, procesadas o gestionadas por una tercera parte. Se recomienda que la organización asegure que se mantenga la visibilidad de las actividades de seguridad como gestión de cambios, identificación de vulnerabilidades y reporte/respuesta de incidentes de seguridad de información a través de un proceso de reportes claro y definido, con formato y estructura.

15.2.2 Control: Gestión de cambios a los servicios del proveedor

Se gestionarán los cambios en la provisión de los servicios, incluyendo el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los sistemas y procesos del negocio involucrados y la revaluación de los riesgos.

El proceso de gestión del cambio de un servicio de tercera parte necesita tener cuenta:

• Los cambios realizados por la organización para implementar:

- mejoras a los servicios corrientes ofrecidos;

- desarrollo de cualquier aplicaciones y sistemas nuevos;

- modificaciones o actualizaciones de las políticas y procedimientos del Organismo;

- nuevos controles para resolver los incidentes de la seguridad de la información y para mejorar la seguridad;

• cambios en los servicios de las terceras partes para implementar:

- cambios y mejoras de las redes;

- uso de nuevas tecnologías;

- adopción de nuevos productos o nuevas versiones/publicaciones;

- nuevas herramientas de desarrollo y ambientes;

- cambios de las ubicaciones físicas de las instalaciones de servicio;

- cambio de los proveedores.

16. Cláusula: Gestión de Incidentes de Seguridad



Generalidades

Existen numerosas amenazas que atentan contra la seguridad de la información, representando riesgos latentes que de materializarse pueden ocasionar incidentes de seguridad.

Los Organismos cuentan con innumerables activos de información, cada uno de los cuales puede encontrarse expuesto a sufrir incidentes de seguridad. Es por ello que resulta sumamente necesario contar con una capacidad de gestión de dichos incidentes que permita comenzar por su detección, llevar a cabo su tratamiento y colaborar en la prevención de futuros incidentes similares.

Objetivo

Garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.

Alcance

La Política definida en este documento se aplica a todo incidente que pueda afectar la seguridad de la información del Organismo.

Responsabilidad

El Comité de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el Responsable de Seguridad de la Información maneje los reportes de incidentes y anomalías de los sistemas. Asimismo, dicho Comité, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

El Responsable de Seguridad de la Información tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados así como su comunicación al Comité de Seguridad de la Información, a los propietarios de la información y al Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC).[3]

Asimismo, el Responsable de Seguridad de la Información y el área de Gestión de Recursos Humanos son responsables de comunicar fehacientemente los procedimientos de Gestión de Incidentes a los empleados y contratados al inicio de la relación laboral.

[3] El Programa Nacional que funciona en el ámbito de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN de la SUBSECRETARIA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS tiene entre sus objetivos brindar respuesta ante incidentes en redes, centralizar y coordinar los esfuerzos para el manejo de los incidentes de seguridad que afecten a los recursos informáticos del Sector Público Nacional.

El Responsable del Área Jurídica participará en el tratamiento de incidentes de seguridad que requieran de su intervención.

Todo el personal del Organismo es responsable de reportar debilidades e incidentes de seguridad que oportunamente se detecten.

Política

16.1 Categoría: Informe de los eventos y debilidades de la seguridad de la información

Objetivo

Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.

16.1.1 Control: Reporte de los eventos de la seguridad de información

Los incidentes relativos a la seguridad serán comunicados a través de las autoridades o canales apropiados tan pronto como sea posible.

Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes.

Dicho procedimiento debe contemplar que ante la detección de un supuesto incidente o violación de la seguridad, el Responsable de Seguridad de la Información sea informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo.

Asimismo, mantendrá al Comité de Seguridad al tanto de la ocurrencia de incidentes de seguridad.

Sin perjuicio de informar a otros Organismos de competencia, el Responsable de Seguridad de la Información, comunicará al Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC) todo incidente o violación de la seguridad, que involucre recursos informáticos.

Todos los empleados y contratistas deben conocer fehacientemente el procedimiento de comunicación de incidentes de seguridad, y deben informar formalmente los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

16.1.2 Control: Reporte de las debilidades de la seguridad

Los usuarios de servicios de información, al momento de tomar conocimiento directo o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar formalmente las mismas al Responsable de Seguridad de la Información.

Se prohíbe expresamente a los usuarios la realización de pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.

16.1.3 Control: Comunicación de Anomalías del Software

Se establecerán procedimientos para la comunicación de anomalías de software, los cuales deben contemplar:

a) Registrar los síntomas del problema y los mensajes que aparecen en pantalla.

b) Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.

c) Alertar inmediatamente de modo formal al Responsable de Seguridad de la Información o del Activo de que se trate.

Se prohíbe a los usuarios quitar el software que supuestamente tiene una anomalía, a menos que estén autorizados formalmente para hacerlo. La recuperación será realizada por personal experimentado, adecuadamente habilitado.

16.2 Categoría: Gestión de los Incidentes y mejoras de la seguridad de la información

Objetivo

Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información.

Se deben establecer las responsabilidades y procedimientos para manejar de manera efectiva los eventos y debilidades en la seguridad de la información una vez que han sido reportados. Se debe aplicar un proceso de mejora continua para la respuesta, monitoreo, evaluación y gestión general de los incidentes en la seguridad de la información.

16.2.1 Control: Responsabilidades y procedimientos

Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad. Se deben considerar los siguientes ítems:

a) Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo como mínimo:

1) Fallas operativas

2) Código malicioso

3) Intrusiones

4) Fraude informático

5) Error humano

6) Catástrofes naturales

b) Comunicar formalmente los incidentes a través de autoridades o canales apropiados tan pronto como sea posible.

c) Contemplar los siguientes puntos en los procedimientos para los planes de contingencia normales (diseñados para recuperar sistemas y servicios tan pronto como sea posible):

1) Definición de las primeras medidas a implementar.

2) Análisis e identificación de la causa del incidente.

3) Planificación e implementación de soluciones para evitar la repetición del mismo, si fuera necesario.

4) Comunicación formal con las personas afectadas o involucradas con la recuperación del incidente.

5) Notificación de la acción a la autoridad y/u Organismos pertinentes.

d) Registrar pistas de auditoría y evidencia similar para:

1) Análisis de problemas internos.

2) Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial (Ver cláusula 10.1. Categoría: Cumplimiento de Requisitos Legales).

e) Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:

1) Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.

2) Documentación de todas las acciones de emergencia emprendidas en forma detallada.

3) Comunicación de las acciones de emergencia al titular de la Unidad Organizativa y revisión de su cumplimiento.

4) Constatación de la integridad de los controles y sistemas del Organismo en un plazo mínimo.

En los casos en los que se considere necesario, se solicitará la participación del Responsable del Área Jurídica del Organismo en el tratamiento de incidentes de seguridad ocurridos.

16.2.2 Control: Aprendiendo a partir de los incidentes de la seguridad de la información

Se definirá un proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes o de alto impacto. Esto será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

16.2.3 Control: Procesos Disciplinarios

Se seguirá el proceso disciplinario formal contemplado en las normas estatutarias, escalafonarias y convencionales que rigen al personal de la Administración Publica Nacional, para los

empleados que violen la Política, Normas y Procedimientos de Seguridad del Organismo (Ver Cláusula 18 Cumplimiento)

17. Cláusula: Gestión de la Continuidad



Generalidades

La administración de la continuidad de las actividades es un proceso crítico que debe involucrar a todos los niveles del Organismo.

El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades del Organismo puedan restablecerse dentro de los plazos requeridos.

Dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades del organismo y asegurar la reanudación oportuna de las operaciones indispensables.

Objetivo

Minimizar los efectos de las posibles interrupciones de las actividades normales del Organismo (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.

Maximizar la efectividad de las operaciones de contingencia del Organismo con el establecimiento de planes que incluyan al menos las siguientes etapas:

a) Notificación/Activación: Consistente en la detección y determinación del daño y la activación del plan.

b) Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.

c) Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

Asegurar la coordinación con el personal del Organismo y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

Alcance

Esta Política se aplica a todos los procesos críticos identificados del Organismo.

Responsabilidad

El Responsable de Seguridad de la Información participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia.

Los Propietarios de la Información y el Responsable de Seguridad de la Información cumplirán las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades del Organismo.

- Evaluar los riesgos para determinar el impacto de dichas interrupciones.

- Identificar los controles preventivos.

- Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del Organismo.

- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades del Organismo.

Los Responsables de Procesos revisarán periódicamente los planes bajo su incumbencia, como así también identificar cambios en las disposiciones relativas a las actividades del Organismo aún no reflejadas en los planes de continuidad.

Los administradores de cada plan verificarán el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad.

El Comité de Seguridad de la Información tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información del Organismo frente a interrupciones imprevistas.

Política

17.1 Categoría: Gestión de continuidad del Organismo

Objetivo

Contraatacar las interrupciones a las actividades del organismo y proteger los procesos críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

17.1.1 Control: Proceso de Administración de la continuidad del Organismo

El Comité de Seguridad de la Información, será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades del Organismo.

Este Comité tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información del Organismo frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

a) Identificar y priorizar los procesos críticos de las actividades del Organismo.

b) Asegurar que todos los integrantes del Organismo comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del Organismo.

c) Elaborar y documentar una estrategia de continuidad de las actividades del Organismo consecuente con los objetivos y prioridades acordados.

d) Proponer planes de continuidad de las actividades del Organismo de conformidad con la estrategia de continuidad acordada.

e) Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.

f) Coordinar actualizaciones periódicas de los planes y procesos implementados.

g) Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades del Organismo.

h) Proponer las modificaciones a los planes de contingencia.

17.1.2 Control: Continuidad de las Actividades y Análisis de los impactos

Con el fin de establecer un Plan de Continuidad de las Actividades del Organismo se deben contemplar los siguientes puntos:

• Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades, por ejemplo, fallas en el equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación, incendio, desastres naturales, destrucción edilicia, atentados, etc.

• Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.

• Identificar los controles preventivos, como por ejemplo sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de backup, los registros no electrónicos vitales, etc.

Esta actividad será llevada a cabo con la activa participación de los propietarios de los procesos y recursos de información de que se trate y el Responsable de Seguridad de la Información, considerando todos los procesos de las actividades del Organismo y no limitándose a las instalaciones de procesamiento de la información.

Según los resultados de la evaluación de esta actividad, se desarrollará un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del Organismo. Una vez que se ha creado este plan, el mismo debe ser propuesto por el Comité de Seguridad de la Información a la máxima autoridad del Organismo para su aprobación.

17.1.3 Control: Elaboración e implementación de los planes de continuidad de las Actividades del Organismo

Los propietarios de procesos y recursos de información, con la asistencia del Responsable de Seguridad de la Información, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades del Organismo. Estos procesos deben ser propuestos por el Comité de Seguridad de la Información.

El proceso de planificación de la continuidad de las actividades considerará los siguientes puntos:

a) Identificar y acordar respecto a todas las funciones y procedimientos de emergencia.

b) Analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.

c) Implementar procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de las dependencias de actividades externas y a los contratos vigentes.

d) Documentar los procedimientos y procesos acordados.

e) Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.

f) instruir al personal involucrado en los procedimientos de reanudación y recuperación en los siguientes temas:

1) Objetivo del plan.

2) Mecanismos de coordinación y comunicación entre equipos (personal involucrado).

3) Procedimientos de divulgación.

4) Requisitos de la seguridad.

5) Procesos específicos para el personal involucrado.

6) Responsabilidades individuales.

g) Probar y actualizar los planes, guardando evidencia formal de las pruebas y sus resultados.

Asimismo, el proceso de planificación debe concentrarse en los objetivos de las actividades requeridas del organismo, por ejemplo, restablecimiento de los servicios a los usuarios en un plazo aceptable. Deben considerarse los servicios y recursos que permitirán que esto ocurra, incluyendo, dotación de personal, recursos que no procesan información, así como acuerdos para reanudación de emergencia en sitios alternativos de procesamiento de la información.

17.1.4 Control: Marco para la Planificación de la Continuidad de las Actividades del Organismo

Se mantendrá un solo marco para los planes de continuidad de las actividades del Organismo, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes.

El administrador de cada plan de continuidad será el encargado de coordinar las tareas definidas en el mismo.

Estas modificaciones deben ser propuestas por el Comité de Seguridad de la Información para su aprobación.

El marco para la planificación de la continuidad de las actividades del Organismo, tendrá en cuenta los siguientes puntos:

a) Prever las condiciones de implementación de los planes que describan el proceso a seguir (cómo evaluar la situación, qué personas estarán involucradas, etc.) antes de poner en marcha los mismos.

b) Definir los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones del Organismo y/o la vida humana. Esto debe incluir disposiciones con respecto a la gestión de las relaciones públicas y a vínculos eficaces a establecer con las autoridades públicas pertinentes, por ejemplo, la policía, bomberos y autoridades locales.

c) Realizar los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales del Organismo o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos en los plazos requeridos.

d) Redactar los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales del Organismo.

e) Definir un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan, y el proceso para el mantenimiento del mismo.

f) Efectuar actividades de concientización e instrucción al personal, diseñadas para propiciar la comprensión de los procesos de continuidad las actividades y garantizar que los procesos sigan siendo eficaces.

g) Documentar las responsabilidades y funciones de las personas, describiendo los responsables de la ejecución de cada uno de los componentes del plan y las vías de contacto posibles. Se deben mencionar alternativas cuando corresponda. Es de suma importancia definir a un responsable de declarar el estado de contingencia, lo cual dará inicio al plan.

Los administradores de los planes de contingencia son:

Plan de Contingencia	Administrador
…………………………..	
…………………………..	

El cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad, deben contarse entre las responsabilidades de los administradores de cada plan. Las disposiciones de emergencia para servicios técnicos alternativos, como instalaciones de comunicaciones o de procesamiento de información, normalmente se cuentan entre las responsabilidades de los proveedores de servicios.

17.1.5 Control: Ensayo, Mantenimiento y Reevaluación de los Planes de continuidad del Organismo

Debido a que los planes de continuidad de las actividades del Organismo pueden fallar, por suposiciones incorrectas, errores o cambios en el equipamiento, se establecen las siguientes pautas de acción:

• El Comité de Seguridad de la Información establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.

• El cronograma indicará quienes son los responsables de llevar a cabo cada una de las pruebas y de elevar el resultado obtenido al citado Comité.

Se deben utilizar diversas técnicas para garantizar que los planes de contingencia funcionarán ante un hecho real, y éstas incluirán por lo menos:

a) Efectuar pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación las actividades utilizando ejemplos de interrupciones).

b) Realizar simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis).

c) Efectuar pruebas de recuperación técnica (garantizando que los sistemas de información puedan ser restablecidos con eficacia).

d) Realizar ensayos completos probando que el Organismo, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.

Para las operaciones críticas del Organismo se tomarán en cuenta, además, los siguientes mecanismos:

a) Efectuar pruebas de recuperación en un sitio alternativo (ejecutando los procesos de las actividades del Organismo en paralelo, con operaciones de recuperación fuera del sitio principal).

b) Realizar pruebas de instalaciones y servicios de proveedores (garantizando que los productos y servicios de proveedores externos cumplan con los compromisos contraídos).

Todas las pruebas efectuadas deben ser documentadas, resguardándose la evidencia formal de la ejecución y de los resultados obtenidos.

Los planes de continuidad de las actividades del Organismo serán revisados y actualizados periódicamente, para garantizar su eficacia permanente. Se incluirán procedimientos en el programa de administración de cambios del Organismo para garantizar que se aborden adecuadamente los tópicos de continuidad de las actividades.

La periodicidad de revisión de los planes de contingencia es la siguiente:

Plan de Contingencia	Revisar cada	Responsable de Revisión

Cada uno de los Responsables de Procesos es el responsable de las revisiones periódicas de cada uno de los planes de continuidad de su incumbencia, como así también de la identificación de cambios en las disposiciones relativas a las actividades del Organismo aún no reflejadas en dichos planes.

Debe prestarse atención, especialmente, a los cambios de:

a) Personal.

b) Direcciones o números telefónicos.

c) Estrategia del Organismo.

d) Ubicación, instalaciones y recursos.

e) Legislación.

f) Contratistas, proveedores y clientes críticos.

g) Procesos, o procesos nuevos / eliminados.

h) Tecnologías.

i) Requisitos operacionales.

j) Requisitos de seguridad.

k) Hardware, software y otros equipos (tipos, especificaciones, y cantidad).

l) Requerimientos de los sitios alternativos.

m) Registros de datos vitales.

Todas las modificaciones efectuadas serán propuestas por el Comité de Seguridad de la Información para su aprobación por el superior jerárquico que corresponda.

Por otra parte, el resultado de este proceso será dado a conocer a fin de que todo el Personal involucrado tenga conocimiento de los cambios incorporados.

17.2 Categoría: Redundancias

Objetivo

Asegurar la continuidad de la información y que esté integrada a los sistemas de gestión.

17.2.1 Control: Disponibilidad de las instalaciones de procesamiento de la información

Se deben implementar las instalaciones de procesamiento de la información con la debida redundancia a efectos de cumplir con los requisitos definidos.

Para cumplir con lo anterior el Organismo debe identificar los requisitos funcionales para considerar los componentes o arquitecturas redundantes. Hay tener en cuenta durante el diseño, la actividad de la gestión de los riesgos de integridad y confidencialidad de la información que puedan acarrear las redundancias.

18. Cláusula: Cumplimiento



Generalidades

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.

Los requisitos normativos y contractuales pertinentes a cada sistema de información deben estar debidamente definidos y documentados.

El Área Jurídica del Organismo, será responsable de encuadrar jurídicamente la formulación e implementación de la política.

Objetivos

Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas al Organismo y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.

Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad del Organismo.

Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.

Determinar los plazos para el mantenimiento de información y para la recolección de evidencia del Organismo.

Alcance

Esta Política se aplica a todo el personal del Organismo, cualquiera sea su situación de revista.

Asimismo se aplica a los sistemas de información, normas, procedimientos, documentación y plataformas técnicas del Organismo y a las auditorías efectuadas sobre los mismos.

Responsabilidad

El Responsable de Seguridad de la Información cumplirá las siguientes funciones:

- Definir normas y procedimientos para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros.

- Realizar revisiones periódicas de todas las áreas del Organismo a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.

- Verificar periódicamente que los sistemas de información cumplan la política, normas y procedimientos de seguridad establecidos.

- Garantizar la seguridad y el control de las herramientas utilizadas para las revisiones de auditoría.

El Responsable del Área Jurídica del Organismo, con la asistencia del Responsable de Seguridad de la Información cumplirán las siguientes funciones:

- Definir y documentar claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información.

- Redactar un Compromiso de Confidencialidad a ser firmado por todo el personal.

Los Responsables de Unidades Organizativas velarán por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos en la presente Política, dentro de su área de responsabilidad.

Todos los empleados de los mandos medios y superiores conocerán, comprenderán, darán a conocer, cumplirán y harán cumplir la presente Política y la normativa vigente.

Política

18.1 Categoría: Cumplimiento de Requisitos Legales

Objetivo

Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.

El diseño, operación, uso y gestión de los sistemas de información pueden estar sujetos a requerimientos de seguridad estatutarios, reguladores y contractuales.

18.1.1 Control: Identificación de la Legislación Aplicable

Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

18.1.2 Control: Derechos de Propiedad Intelectual

Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

Los empleados únicamente podrán utilizar material autorizado por el Organismo.

El Organismo solo podrá autorizar el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

La infracción a estos derechos puede tener como resultado acciones legales que podrían derivar en demandas penales.

Se deben tener presentes las siguientes normas:

• Ley de Propiedad Intelectual N° 11.723: Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales.

• Ley de Marcas N° 22.362: Protege la propiedad de una marca y la exclusividad de su uso.

• Ley de Patentes de Invención y Modelos de Utilidad N° 24.481: Protege el derecho del titular de la patente de invención a impedir que terceros utilicen su producto o procedimiento.

Derecho de Propiedad intelectual del Software

El software es considerado una obra intelectual que goza de la protección de la Ley 11.723 de Propiedad Intelectual.

Esta Ley establece que la explotación de la propiedad intelectual sobre los programas de computación incluirá, entre otras formas, los contratos de licencia para su uso o reproducción.

Los productos de software se suministran normalmente bajo acuerdos de licencia que suelen limitar el uso de los productos al equipamiento específico y su copia a la creación de copias de resguardo solamente.

El Responsable de Seguridad de la Información, con la asistencia del Área Jurídica, analizará los términos y condiciones de la licencia, e implementará los siguientes controles:

a) Definir normas y procedimientos para el cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software.

b) Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Propiedad Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las infrinja.

c) Mantener un adecuado registro de activos.

d) Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.

e) Implementar controles para evitar el exceso del número máximo permitido de usuarios.

f) Verificar que sólo se instalen productos con licencia y software autorizado.

g) Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.

h) Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.

i) Utilizar herramientas de auditoría adecuadas.

j) Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

18.1.3 Control: Protección de los Registros del Organismo

Los registros críticos del Organismo se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales del Organismo.

Los registros se clasificarán en diferentes tipos, por ejemplo registros contables, registros de base de datos, registros de auditoría y procedimientos operativos, cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento, por ejemplo papel, microfichas, medios magnéticos u ópticos.

Tipo de Registro	Siste ma de Inform ación	Perío do de Reten ción	Medio de Almacen amiento	Respons able

Las claves criptográficas asociadas con archivos cifrados se mantendrán en forma segura y estarán disponibles para su uso por parte de personas autorizadas cuando resulte necesario.

Se debe considerar la posibilidad de degradación de los medios utilizados para el almacenamiento de los registros. Los procedimientos de almacenamiento y manipulación se implementarán de acuerdo con las recomendaciones del fabricante.

Si se seleccionan medios de almacenamiento electrónicos, se incluirán los procedimientos para garantizar la capacidad de acceso a los datos (tanto legibilidad de formato como medios) durante todo el período de retención, a fin de salvaguardar los mismos contra eventuales pérdidas ocasionadas por futuros cambios tecnológicos.

Los sistemas de almacenamiento de datos serán seleccionados de modo tal que los datos requeridos puedan recuperarse de una manera que resulte aceptable para un tribunal de justicia, por ejemplo que todos los registros requeridos puedan recuperarse en un plazo y un formato aceptable.

El sistema de almacenamiento y manipulación garantizará una clara identificación de los registros y de su período de retención legal o normativa. Asimismo, se permitirá una adecuada destrucción de los registros una vez transcurrido dicho período, si ya no resultan necesarios para el Organismo.

A fin de cumplir con estas obligaciones, se tomarán las siguientes medidas:

a) Elaborar y divulgar los lineamientos para la retención, almacenamiento, manipulación y eliminación de registros e información.

b) Preparar un cronograma de retención identificando los tipos esenciales de registros y el período durante el cual deben ser retenidos.

c) Mantener un inventario de programas fuentes de información clave.

d) Implementar adecuados controles para proteger la información y los registros esenciales contra pérdida, destrucción y falsificación.

En particular, se deben tener presente las siguientes normas:

• Ética en el Ejercicio de la Función Pública. Ley 25.188: Establece que las personas que se desempeñen en la función pública deben proteger y conservar la propiedad del Estado y sólo emplear sus bienes con los fines autorizados.

• Código de Ética de la Función Pública: Dispone que el funcionario público debe proteger y conservar los bienes del Estado y utilizar los que le fueran asignados para el desempeño de sus funciones de manera racional, evitando su abuso, derroche o desaprovechamiento.

• Código Penal Art. 255: Sanciona a quien sustrajere, ocultare, destruyere o inutilizare objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario o de otra persona en el interés del servicio público. Si el culpable fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

• Ley N° 24.624. Artículo 30: Autoriza el archivo y la conservación en soporte electrónico u óptico indeleble de la documentación financiera, de personal y de control de la Administración Pública Nacional y otorga valor jurídico y probatorio a la documentación existente que se incorpore al Archivo General de la Administración, mediante la utilización de tecnología que garantice la estabilidad, perdurabilidad, inmutabilidad e inalterabilidad del soporte de guarda físico de la mencionada documentación.

• Decisión Administrativa 43/96: Reglamenta el Art. 30 de la Ley 24.624. Determina su ámbito de aplicación, define conceptos y precisa los requisitos de carácter general, los relacionados con los documentos en particular y con el soporte a utilizar en la redacción, producción o reproducción de aquellos.

• Ley de Propiedad Intelectual N° 11.723: Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo las compilaciones de datos o de otros materiales.

• Ley N° 25.506: Establece que la exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.

• Código Penal: Sanciona a aquel que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos (Art. 183).

18.1.4 Control: Protección de Datos y Privacidad de la Información Personal

Todos los empleados deben conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

El Organismo redactará un “Compromiso de Confidencialidad”, el cual debe ser suscrito por todos los funcionarios públicos y contratistas. La copia firmada del compromiso será retenida en forma segura por el Organismo.

Mediante este instrumento el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del Responsable del Activo de que se trate. A través del “Compromiso de Confidencialidad” se debe advertir al empleado que determinadas actividades pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

En particular, se deben tener presente las siguientes normas:

• Ley Marco de Regulación de Empleo Público Nacional. Ley 25.164: Establece que los Funcionarios Públicos deben observar el deber de fidelidad que se derive de la índole de las tareas que le fueron asignadas y guardar la discreción correspondiente o la reserva absoluta, en su caso, de todo asunto del servicio que así lo requiera.

• Convenio Colectivo de Trabajo General: Dispone que todos los agentes deben observar el deber de fidelidad que se derive de la índole de las tareas que le fueran asignadas y guardar la discreción correspondiente, con respecto a todos los hechos e informaciones de los cuales tenga conocimiento en el ejercicio o con motivo del ejercicio de sus funciones.

• Ética en el Ejercicio de la Función Pública. Ley 25.188: Obliga a todas las personas que se desempeñen en la función pública a abstenerse de utilizar información adquirida en el cumplimiento de sus funciones para realizar actividades no relacionadas con sus tareas oficiales o de permitir su uso en beneficio de intereses privados.

• Código de Ética de la Función Pública: Establece que el funcionario público debe abstenerse de difundir toda información que hubiera sido calificada como reservada o secreta conforme a las disposiciones vigentes, ni la debe utilizar, en beneficio propio o de terceros o para fines ajenos al servicio, información de la que tenga conocimiento con motivo o en ocasión del ejercicio de sus funciones y que no esté destinada al público en general.

• Protección de Datos Personales. Ley 25.326: Establece responsabilidades para aquellas personas que recopilan, procesan y divulgan información personal y define criterios para procesar datos personales o cederlos a terceros.

• Confidencialidad. Ley N° 24.766: Impide la divulgación a terceros, o su utilización sin previo consentimiento y de manera contraria a los usos comerciales honestos, de información secreta y con valor comercial que haya sido objeto de medidas razonables para mantenerla secreta.

• Código Penal: Sanciona a aquel que abriere o accediere indebidamente a una comunicación electrónica o indebidamente la suprimiere o desviare (Art. 153), al que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido (Art. 153 bis), al que el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros. (Art. 155), al que teniendo noticias de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa (Art. 156), al funcionario público que revelare hechos, actuaciones o documentos que por la ley deben quedar secretos (Art. 157), al que a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales, ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley e ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales (Art. 157 bis), al que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos (Art. 183), al que revelare secretos políticos o militares concernientes a la seguridad, a los medios de defensa o a las relaciones exteriores de la Nación, o al que por imprudencia o negligencia diere a conocer los secretos mencionados anteriormente, de los que se hallare en posesión en virtud de su empleo u oficio (Art. 222 y 223).

Asimismo, debe considerarse lo establecido en el Decreto 1172/03, que regula el acceso a la información pública por parte de los ciudadanos.

18.1.5 Control: Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información

Los recursos de procesamiento de información del Organismo se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido.

Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

En particular, se debe respetar lo dispuesto por las siguientes normas:

• Ley Marco de Regulación de Empleo Público Nacional. Ley 25.164: Prohíbe hacer uso indebido o con fines particulares del patrimonio estatal.

• Convenio Colectivo de Trabajo General: Obliga a los agentes a no hacer uso indebido o con fines particulares del patrimonio estatal.

• Ética en el Ejercicio de la Función Pública. Ley 25.188: Obliga a las personas que se desempeñen en la función pública a proteger y conservar la propiedad del Estado y sólo emplear sus bienes con los fines autorizados.

• Código de Ética de la Función Pública: Obliga al funcionario público a proteger y conservar los bienes del Estado y utilizar los que le fueran asignados para el desempeño de sus funciones de manera racional, evitando su abuso, derroche o desaprovechamiento.

• Código Penal: Sanciona a aquel que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños (Art. 183).

18.1.6 Control: Regulación de Controles para el Uso de Criptografía

Al utilizar firmas digitales o electrónicas, se debe considerar lo dispuesto por la Ley 25.506 y su decreto reglamentario Decreto 2628/02, que establecen las condiciones bajo las cuales una firma digital es legalmente válida.

Respecto a la comercialización de controles criptográficos, nuestro país ha suscrito el acuerdo Wassennar, que establece un listado de materiales y tecnologías de doble uso, cuya comercialización puede ser considerada peligrosa.

El Decreto 603/92 regula el Régimen de Control de las Exportaciones Sensitivas y de Material Bélico, estableciendo un tratamiento especial para la exportación de determinados bienes que pueden ser comprendidos dentro del concepto de material bélico.

Se debe obtener asesoramiento antes de transferir a otro país información cifrada o controles criptográficos. Para ello se puede consultar a la Dirección General de Política, de la Secretaría de Asuntos Militares, Ministerio de Defensa, a fin de saber si el material exportable requiere algún tratamiento especial.

18.1.7 Control: Recolección de Evidencia

Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos.

Cuando la acción implique la aplicación de una ley, la evidencia presentada debe cumplir con lo establecido por las normas procesales. Para lograr la validez de la evidencia, el Organismo garantizará que sus sistemas de información cumplen con la normativa y los estándares o códigos de práctica relativos a la producción de evidencia válida.

Para lograr la calidad y totalidad de la evidencia es necesaria una sólida pista de la misma. Esta pista se establecerá cumpliendo las siguientes condiciones:

a) Almacenar los documentos en papel originales en forma segura y mantener registros acerca de quién lo halló, dónde se halló, cuándo se halló y quién presenció el hallazgo. Cualquier investigación debe garantizar que los originales no sean alterados.

b) Copiar la información para garantizar su disponibilidad. Se mantendrá un registro de todas las acciones realizadas durante el proceso de copia. Se almacenará en forma segura una copia de los medios y del registro.

Cuando se detecta un incidente, puede no resultar obvio si éste derivará en una demanda legal por lo tanto se deben tomar todos los recaudos establecidos para la obtención y preservación de la evidencia.

Se debe tener presente lo dispuesto por el Reglamento de Investigaciones Administrativas, procedimiento administrativo especial, de naturaleza correctiva interna que constituye garantía suficiente para la protección de los derechos y correcto ejercicio de las responsabilidades impuestas a los agentes públicos. Este Decreto debe ser complementado por lo dispuesto en la Ley N° 19.549 (Ley de Procedimientos Administrativos) y por toda otra normativa aplicable, incluido el Código Penal, el que sanciona a quien sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público (Art. 255).

18.1.8 Control: Delitos Informáticos

Todos los empleados deben conocer la existencia de la Ley 26.388 de Delitos Informáticos, a partir de cuyo dictado se castigan penalmente ciertas conductas cometidas mediante medios informáticos. En tal sentido, los agentes públicos deben conocer con exactitud el alcance de los nuevos tipos penales introducidos por la norma mencionada.

Cabe señalar que la mayoría de las conductas descritas por dicha norma vinculada ya han sido señaladas en los apartados precedentes.

18.2 Categoría: Revisiones de la Política de Seguridad y la Compatibilidad Técnica

Objetivo

Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.

La seguridad de los sistemas de información se debiera revisar regularmente.

Estas revisiones deben realizarse en base a las políticas de seguridad apropiadas y las plataformas técnicas, y los sistemas de información deben ser auditados en cumplimiento con los estándares de implementación de seguridad aplicables y los controles de seguridad documentados.

18.2.1 Control: Cumplimiento de la Política de Seguridad

Cada Responsable de Unidad Organizativa, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

El Responsable de Seguridad de la Información, realizará revisiones periódicas de todas las áreas del Organismo a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

a) Sistemas de información.

b) Proveedores de sistemas.

c) Propietarios de información.

d) Usuarios.

Los Propietarios de la Información brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

18.2.2 Control: Verificación de la Compatibilidad Técnica

El Responsable de Seguridad de la Información verificará periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. En caso de ser necesario, estas revisiones contemplarán la asistencia técnica especializada.

El resultado de la evaluación se volcará en un informe técnico para su ulterior interpretación por parte de los especialistas. Para ello, la tarea podrá ser realizada por un profesional experimentado (en forma manual o con el apoyo de herramientas de software), o por un paquete de software automatizado que genere reportes que serán interpretados por un especialista técnico.

La verificación del cumplimiento comprenderá pruebas de penetración y tendrá como objetivo la detección de vulnerabilidades en el sistema y la verificación de la eficacia de los controles con relación a la prevención de accesos no autorizados. Se tomarán los recaudos necesarios en el caso de pruebas de penetración exitosas que comprometan la seguridad del sistema.

Las verificaciones de cumplimiento sólo serán realizadas por personas competentes, formalmente autorizadas y bajo la supervisión.

18.3 Categoría: Consideraciones de Auditorías de Sistemas

Objetivo

Maximizar la efectividad de y minimizar la interferencia desde/hacia el proceso de auditoría del sistema de información.

Durante las auditorías de los sistemas de información debieran existir controles para salvaguardar los sistemas operacionales y herramientas de auditoría.

Con relación a las auditorías, serán de aplicación las Normas de Control Interno para Tecnologías de Información, aprobadas por la resolución SIGEN N° 48/05.

18.3.1 Controles de Auditoría de Sistemas

Cuando se realicen actividades de auditoría que involucren verificaciones de los sistemas en producción, se tomarán recaudos en la planificación de los requerimientos y tareas, y se acordará con las áreas involucradas a efectos de minimizar el riesgo de interrupciones en las operaciones.

Se contemplarán los siguientes puntos:

a) Acordar con el Área que corresponda los requerimientos de auditoría.

b) Controlar el alcance de las verificaciones. Esta función será realizada por el responsable de auditoría.

c) Limitar las verificaciones a un acceso de sólo lectura del software y datos de producción. Caso contrario, se tomarán los resguardos necesarios a efectos de aislar y contrarrestar los efectos de las modificaciones realizadas, una vez finalizada la auditoría. Por ejemplo:

• Eliminar archivos transitorios.

• Eliminar entidades ficticias y datos incorporados en archivos maestros.

• Revertir transacciones.

• Revocar privilegios otorgados

d) Identificar claramente los recursos de tecnologías de información (TI) para llevar a cabo las verificaciones, los cuales serán puestos a disposición de los auditores. A tal efecto, la Unidad de Auditoría o en su defecto quien sea propuesto por el Comité de Seguridad de la Información completará el siguiente formulario, el cual debe ser puesto en conocimiento de las áreas involucradas:

Recursos de TI a utilizar en la Verificación	
Sistemas de información	....
Base de datos	....
Hardware	....
Software de Auditoría	....
Medios Magnéticos	....
Personal de Auditoría	....
Interlocutores de las Áreas de Informática	....
Interlocutores de las Áreas Usuarias	....
Conexiones a Red	....
....	....

e) Identificar y acordar los requerimientos de procesamiento especial o adicional.

f) Monitorear y registrar todos los accesos, a fin de generar una pista de referencia. Los datos a resguardar deben incluir como mínimo:

• Fecha y hora.

• Puesto de trabajo.

• Usuario.

• Tipo de acceso.

• Identificación de los datos accedidos.

• Estado previo y posterior.

• Programa y/o función utilizada.

g) Documentar todos los procedimientos de auditoría, requerimientos y responsabilidades.

18.3.2 Control: Protección de los Elementos Utilizados por la Auditoría de Sistemas

Se protegerá el acceso a los elementos utilizados en las auditorías de sistemas, o sea archivos de datos o software, a fin de evitar el mal uso o el compromiso de los mismos.

Dichas herramientas estarán separadas de los sistemas en producción y de desarrollo, y se les otorgará el nivel de protección requerido.

Se tomarán los recaudos necesarios a efectos de cumplimentar las normas de auditoría dispuestas por la Sindicatura General de la Nación.

18.3.3 Control: Sanciones Previstas por Incumplimiento

Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente Política de Seguridad conforme a lo dispuesto por las normas estatutarias, escalafonarias y convencionales que rigen al personal de la Administración Pública Nacional, y en caso de corresponder, se realizarán las acciones correspondientes ante el o los Organismos pertinentes.

Las sanciones sólo pueden imponerse mediante un acto administrativo que así lo disponga cumpliendo las formalidades impuestas por los preceptos constitucionales, la Ley de Procedimiento Administrativo y demás normativas específicas aplicables.

Amén de las sanciones disciplinarias o administrativas, el agente que no da debido cumplimiento a sus obligaciones pueden incurrir también en responsabilidad civil o patrimonial —cuando ocasiona un daño que debe ser indemnizado— y/o en responsabilidad penal —cuando su conducta constituye un comportamiento considerado delito por el Código Penal y leyes especiales.

e. 25/02/2015 N° 11885/15 v. 25/02/2015